

Linear Precoder Design for a MIMO Gaussian Wiretap Channel with Full-Duplex Source and Destination Nodes

Lingxiang Li, Zhi Chen, *Member, IEEE*,
Athina P. Petropulu, *Fellow, IEEE*, and Jun Fang, *Member, IEEE*

Abstract—We consider linear precoder design for a multiple-input multiple-output (MIMO) Gaussian wiretap channel, which comprises two legitimate nodes, i.e., *Alice* and *Bob*, operating in Full-Duplex (FD) mode and exchanging confidential messages in the presence of a passive eavesdropper. Using the sum secrecy degrees of freedoms (sum S.D.o.F.) as reliability measure, we formulate an optimization problem with respect to the precoding matrices. In order to solve this problem, we first propose a cooperative secrecy transmission scheme, and prove that its feasible set is sufficient to achieve the maximum sum S.D.o.F.. Based on that feasible set, we then determine the maximum achievable sum S.D.o.F. in closed form, and provide a method for constructing the precoding matrix pair which achieves the maximum sum S.D.o.F.. Results show that, the FD based network provides an attractive secrecy transmission rate performance.

Index Terms—Physical-layer security, Cooperative communications, Multi-input Multi-output, Full-duplex.

I. INTRODUCTION

Full-duplex (FD) has attracted intensive attention in the past few years since it has the potential to double the spectral efficiency. Due to the challenges in suppressing self-interference, which is inherent to FD, wireless communication systems have largely avoided FD up to recently. However, as short-range systems with low-power transmitters such as small-cell systems and WiFi are becoming dominant, there has been renewed interest in FD, since self-interference in such systems is more manageable [1], [2].

Recently, FD nodes were used in the context of physical layer secrecy. One line of research considers an FD receiver (*Bob*) [3]–[5], who transmits jamming signals, which overlap in time and frequency with the source’s (*Alice*) signal. Introducing jamming signals in the form of artificial noise is an effective way to improve secrecy [6]–[14], since jamming signals can be designed to degrade the eavesdropper’s (*Eve*) channel without hurting the legitimate channel. Typically, the jamming signals are transmitted by the transmitter [6], [7], or from external helpers [8]–[14]. Jamming by the transmitter does not have to rely on external helpers, who may not be trustworthy, or maybe be moving and thus hard to keep track

of. Multi-antenna techniques have been used to further boost the potential benefits of using an FD *Bob*. Specifically, [15]–[17] proposed algorithms for maximizing the secrecy rate over the covariance matrix of jamming signals, while [18] studied the maximum secrecy degrees of freedom (S.D.o.F.), and uncovered its connection to the number of antennas at each node.

Using an FD transmitter as well as an FD receiver has the potential to substantially improve the achievable secrecy rate. Further, when both transmitter and receiver have multiple antennas, the transmission of a given node during the reception of information can be designed to act as jamming signal and degrade *Eve*’s channel. This is considered in [19]–[21], where the bidirectional communication creates co-channel interference (CCI), which can act as an alternative to jamming for the purpose of degrading *Eve*’s channel [22]–[28]. In particular, the works [19], [20] assumed that each terminal receives with a single antenna, and proposed algorithms to find a beamforming design that maximizes the achievable secrecy rate; the work of [21] assumed that each terminal transmits and receives with multiple antennas, and proposed algorithms to find the beamforming design that minimizes the transmit power subject to certain quality of service (QoS) requirements.

In this paper, we consider the general multi-input and multi-output (MIMO) Gaussian wiretap channel as in [21], i.e., a network comprising two FD legitimate nodes *Alice* and *Bob*, and a passive eavesdropper *Eve*. Unlike [21], which assumes that each transmitter sends a single signal stream and tries to minimize the transmit power subject to certain QoS requirements, we consider the multiple signal streams case and our goal is to maximize the achievable sum secrecy rate via the proper design of precoding matrices. Due to the self-interference, the achievable secrecy rate of each link is a nonlinear fractional function of the precoding matrices. This makes the sum secrecy rate maximization problem a difficult problem to solve. Instead, we consider the sum S.D.o.F. as a surrogate, i.e., the rate at which the achievable sum secrecy rate scales with $\log(P)$ in the high signal-to-noise ratio (SNR) regime.

Our main contributions are summarized below.

We propose a design for the precoding matrices of *Alice* and *Bob*, with which the maximum sum S.D.o.F. is achieved. This is achieved in the following steps. First, we propose a cooperative secrecy transmission scheme, in which the message signals from *Alice* and *Bob* are aligned along the

Lingxiang Li and Zhi Chen and Jun Fang are with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mails: lingxiang.li@rutgers.edu; {chenzhi, JunFang}@uestc.edu.cn). The work was performed when L. Li was a visiting student at Rutgers University.

A. P. Petropulu is with the Department of Electrical and Computer Engineering, Rutgers–The State University of New Jersey, New Brunswick, NJ 08854 USA (e-mail: athinap@rci.rutgers.edu).

same received subspace of *Eve*. We then prove that the maximum sum S.D.o.F. can be achieved by the precoding matrices that include the largest possible number of precoding vectors produced by the proposed scheme, which are linearly independent and interference free. Subsequently, we divide the candidate precoding vector pairs into several subsets, based on their potential to achieve a greater sum S.D.o.F.. For each subset, we provide the number of linearly independent pairs and their mathematical description. Finally, we give an algorithm (see Table II) for selecting the precoding pairs from the various subsets, so that the sum S.D.o.F. is maximized. We also determine the maximum achievable sum S.D.o.F. as a function of the number of antennas (see equations (38)-(41)). Our analytical results show exactly how the sum secrecy rate depends on the number of antennas at *Alice*, *Bob* and *Eve*.

In [24], we determined the maximum achievable S.D.o.F. region of a two-user wiretap channel with a source destination pair exchanging confidential messages, another pair exchanging public messages, and a passive eavesdropper who is interested in the communications of the former pair. In this paper, while the methodology is similar to that of [24], the problem is different because, unlike [24], in this paper, *Eve* has interest in both source signals. This makes the S.D.o.F. region maximization problem significantly more difficult. In particular, the problem becomes equivalent to two nonlinear fractional problems (each corresponding to the secrecy rate of a wiretap channel). Therefore, the S.D.o.F. region maximization problem is more complicated and the result cannot be obtained through a straightforward extension of [24].

The rest of this paper is organized as follows. In Section II, we describe the system model and formulate the sum S.D.o.F. maximization problem. In Section III, we propose a secrecy cooperative transmission scheme, and prove that its feasible set is sufficient to achieve the maximum sum S.D.o.F.. In Section IV, we divide the feasible set of precoding vectors into several subsets. For each subset, we derive the formulas of the precoding vectors and determine the number of linearly independent candidate precoding vectors. In Section V, we give the maximum achievable sum S.D.o.F. as a function of the number of antennas, and we also provide a method for constructing the precoding matrix pair which achieves the maximum sum S.D.o.F.. Numerical results are given in Section VI and conclusions are drawn in Section VII.

Notation: $x \sim \mathcal{CN}(0, \Sigma)$ means x is a random variable following a complex circular Gaussian distribution with mean zero and covariance Σ ; $\lfloor a \rfloor$ denotes the largest integer which is less or equal to a ; $(a)^+ \triangleq \max\{a, 0\}$; $\min^+\{a, b\} \triangleq (\min\{a, b\})^+$. We use lower case bold to denote vectors; $\mathbb{C}^{N \times M}$ indicates a $N \times M$ complex matrix set; \mathbf{A}^T , \mathbf{A}^H , $\text{tr}\{\mathbf{A}\}$, $\text{rank}\{\mathbf{A}\}$, and $|\mathbf{A}|$ stand for the transpose, hermitian transpose, trace, rank and determinant of the matrix \mathbf{A} , respectively; $\mathbf{A}(:, j)$ indicates the j -th column of \mathbf{A} ; $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{A})^\perp$ are the subspace spanned by the columns of \mathbf{A} and its orthogonal complement, respectively; $\dim\{\text{span}(\mathbf{A})\}$ represents the number of dimension of the subspace spanned by the columns of \mathbf{A} ; $\text{null}(\mathbf{A})$ denotes the null space of \mathbf{A} ; $\Gamma(\mathbf{A})$ denotes the orthogonal basis of $\text{null}(\mathbf{A})$; \mathbf{A}^\perp denotes the orthogonal basis of $\text{null}(\mathbf{A}^H)$; $\text{span}(\mathbf{A}) \cap \text{span}(\mathbf{B})$ denotes

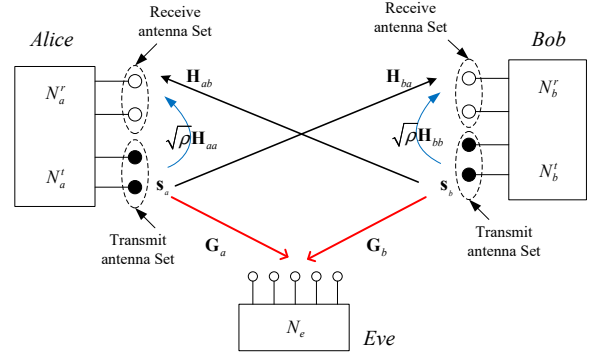


Fig. 1: A MIMO FD bidirectional wiretap channel.

the intersection of the subspaces $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{B})$; $\text{span}(\mathbf{A}) \setminus \text{span}(\mathbf{B}) \triangleq \{\mathbf{x} | \mathbf{x} \in \text{span}(\mathbf{A}), \mathbf{x} \notin \text{span}(\mathbf{B})\}$. \mathbf{I} represents an identity matrix with appropriate size. We denote by $\mathcal{I} \succ \mathcal{J}$ to indicate that we pick precoding vector pairs from \mathcal{I} prior to \mathcal{J} ; we denote by $\mathcal{I} = \mathcal{J}$ to indicate that we can select precoding vector pairs from \mathcal{I} and \mathcal{J} without any specific constraints on rankings.

II. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a MIMO Gaussian wiretap channel (see Fig. 1), which consists of two legitimate transceivers, *Alice* and *Bob*, who want to exchange information, and an external passive eavesdropper, *Eve*, who has interest in the message signals sent by both *Alice* and *Bob*. *Alice* and *Bob* are equipped with N_a and N_b antennas, respectively. *Eve* is equipped with N_e antennas. To enable simultaneous information exchange, both *Alice* and *Bob* operate in FD mode, i.e., each of them is equipped with two groups of RF chains and corresponding antennas, one for transmitting and one for receiving. Specifically, *Alice* allocates N_a^r antennas to receive and the remaining $N_a^t = N_a - N_a^r$ antennas to transmit. *Bob* allocates N_b^r antennas to receive and the remaining $N_b^t = N_b - N_b^r$ antennas to transmit. We denote by $\mathbf{s}_a \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{s}_b \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ the message signals sent by *Alice* and *Bob*, respectively. Both signals are transmitted simultaneously and over the same frequency spectrum. Such transmission leads to self-interference, e.g., *Bob* will also see the signals sent from its own transmit antennas, i.e., \mathbf{s}_b , whose intended receiver is *Alice*. There are various self-interference cancellation techniques such as antenna isolation, analog-circuit-domain based methods and digital-domain based methods, however, today's state-of-the-art cannot achieve full self-interference cancellation [1]. To describe the effect of residual self-interference we employ the loop interference model as in [15], with parameter $\rho = 0$ corresponding to the no residual self-interference case and $0 < \rho \leq 1$ corresponding to different residual self-interference levels. The signal received at *Alice* and *Bob* can thus be expressed respectively as

$$\mathbf{y}_a = \sqrt{\rho} \mathbf{H}_{aa} \mathbf{V}_a \mathbf{s}_a + \mathbf{H}_{ab} \mathbf{V}_b \mathbf{s}_b + \mathbf{n}_a, \quad (1a)$$

$$\mathbf{y}_b = \mathbf{H}_{ba} \mathbf{V}_a \mathbf{s}_a + \sqrt{\rho} \mathbf{H}_{bb} \mathbf{V}_b \mathbf{s}_b + \mathbf{n}_b. \quad (1b)$$

The signal received at *Eve* can be expressed as

$$\mathbf{y}_e = \mathbf{G}_a \mathbf{V}_a \mathbf{s}_a + \mathbf{G}_b \mathbf{V}_b \mathbf{s}_b + \mathbf{n}_e. \quad (2)$$

Here, \mathbf{V}_a and \mathbf{V}_b are the precoding matrices at *Alice* and *Bob*, respectively; $\mathbf{n}_a \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, $\mathbf{n}_b \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ are independent AWGN vectors, and represent the measurement noise at *Alice*, *Bob* and *Eve*, respectively; $\mathbf{H}_{ba} \in \mathbb{C}^{N_b^r \times N_a^t}$ denotes the channel matrix from *Alice* to *Bob*; $\mathbf{H}_{ab} \in \mathbb{C}^{N_a^r \times N_b^t}$ denotes the channel matrix from *Bob* to *Alice*; $\mathbf{H}_{aa} \in \mathbb{C}^{N_a^r \times N_a^t}$ and $\mathbf{H}_{bb} \in \mathbb{C}^{N_b^r \times N_b^t}$ are self-interfering matrices; $\mathbf{G}_a \in \mathbb{C}^{N_e \times N_a^t}$ and $\mathbf{G}_b \in \mathbb{C}^{N_e \times N_b^t}$ denote the channel matrix from *Alice* and *Bob* to *Eve*, respectively.

In this paper, we make the following assumptions:

- 1) The messages s_a and s_b are independent of each other, and independent of the noise vectors. The receivers do not have the capability of multiple-user decoding and they will treat the interference simply as noise.
- 2) All the channels are flat fading and independent of each other; the corresponding channel matrices are full rank. Global channel state information (CSI) is available at the legitimate nodes, including the CSI of *Eve*. This is possible in situations in which *Eve* is a passive network user and its whereabouts and behavior can be monitored.

For a given precoding matrix pair $(\mathbf{V}_a, \mathbf{V}_b)$, the maximum achievable rate at the legitimate receiver and the eavesdropper can be respectively expressed as [29]

$$R_a = \log|\mathbf{I} + (\mathbf{I} + \rho \mathbf{H}_{bb} \mathbf{Q}_b \mathbf{H}_{bb}^H)^{-1} \mathbf{H}_{ba} \mathbf{Q}_a \mathbf{H}_{ba}^H|, \quad (3a)$$

$$R_b = \log|\mathbf{I} + (\mathbf{I} + \rho \mathbf{H}_{aa} \mathbf{Q}_a \mathbf{H}_{aa}^H)^{-1} \mathbf{H}_{ab} \mathbf{Q}_b \mathbf{H}_{ab}^H|, \quad (3b)$$

$$R_e^a = \log|\mathbf{I} + (\mathbf{I} + \mathbf{G}_b \mathbf{Q}_b \mathbf{G}_b^H)^{-1} \mathbf{G}_a \mathbf{Q}_a \mathbf{G}_a^H|, \quad (3c)$$

$$R_e^b = \log|\mathbf{I} + (\mathbf{I} + \mathbf{G}_a \mathbf{Q}_a \mathbf{G}_a^H)^{-1} \mathbf{G}_b \mathbf{Q}_b \mathbf{G}_b^H|, \quad (3d)$$

where $\mathbf{Q}_a \triangleq \mathbf{V}_a \mathbf{V}_a^H$ and $\mathbf{Q}_b \triangleq \mathbf{V}_b \mathbf{V}_b^H$ denote the transmit covariance matrices of *Alice* and *Bob*, respectively.

Correspondingly, the achievable S.D.o.F. is [30]

$$d_s^i \triangleq \lim_{P \rightarrow \infty} R_s^i / \log P, \quad i = a, b, \quad (4)$$

where P denotes the transmit power budget, R_s^i the secrecy rate which equals

$$R_s^i \triangleq (R_i - R_e^i)^+. \quad (5)$$

Let the maximum achievable sum S.D.o.F. over the precoding matrices be

$$d_s^{\text{sum}} \triangleq \max_{(\mathbf{V}_a, \mathbf{V}_b) \in \mathcal{I}} (d_s^a + d_s^b), \quad (6)$$

with $\mathcal{I} \triangleq \{(\mathbf{V}_a, \mathbf{V}_b) | \text{tr}\{\mathbf{V}_a \mathbf{V}_a^H\} = P, \text{tr}\{\mathbf{V}_b \mathbf{V}_b^H\} = P\}$. In this paper, we aim to determine d_s^{sum} as a function of the number of antennas, and thus provide some insight into the potential benefits that can be brought by FD operations. To that objective, in the following sections, we will first introduce a cooperative transmission scheme which can achieve the maximum sum S.D.o.F.. Subsequently, by studying the cooperative transmission scheme, we will determine d_s^{sum} in closed form and also provide the precoding matrix pair which achieves the sum S.D.o.F. of d_s^{sum} .

III. COOPERATIVE SECRECY TRANSMISSION SCHEME

Before proceeding, please refer to Appendix A for some mathematical background on generalized singular value decomposition (GSVD), which provides a mathematical basis for the text to follow.

Lemma 1: For any given precoding matrices $(\mathbf{V}_a, \mathbf{V}_b) \in \mathcal{I}$ the achieved S.D.o.F. can be re-expressed as follows:

$$d_s^a(\mathbf{V}_a, \mathbf{V}_b) = m_1(\mathbf{V}_a, \mathbf{V}_b) - n_1(\mathbf{V}_a, \mathbf{V}_b), \quad (7a)$$

$$d_s^b(\mathbf{V}_a, \mathbf{V}_b) = m_2(\mathbf{V}_a, \mathbf{V}_b) - n_2(\mathbf{V}_a, \mathbf{V}_b), \quad (7b)$$

in which

$$m_1(\mathbf{V}_a, \mathbf{V}_b) \triangleq \dim\{\text{span}(\mathbf{H}_{ba} \mathbf{V}_a) \setminus \text{span}(\mathbf{H}_{bb} \mathbf{V}_b)\},$$

$$n_1(\mathbf{V}_a, \mathbf{V}_b) \triangleq \dim\{\text{span}(\mathbf{G}_a \mathbf{V}_a) \setminus \text{span}(\mathbf{G}_b \mathbf{V}_b)\},$$

$$m_2(\mathbf{V}_a, \mathbf{V}_b) \triangleq \dim\{\text{span}(\mathbf{H}_{ab} \mathbf{V}_b) \setminus \text{span}(\mathbf{H}_{aa} \mathbf{V}_a)\},$$

$$n_2(\mathbf{V}_a, \mathbf{V}_b) \triangleq \dim\{\text{span}(\mathbf{G}_b \mathbf{V}_b) \setminus \text{span}(\mathbf{G}_a \mathbf{V}_a)\}.$$

Proof: The proof is omitted since it's similar to that of the equation (13a) in [24]. ■

With *Lemma 1*, one can see that the achievable S.D.o.F. each legitimate channel can offer, is equal to the dimension difference of the interference free subspaces which the intended destination and *Eve* can respectively see. Motivated by this observation, we propose a cooperative secrecy transmission scheme in which the message signals from *Alice* and *Bob* are aligned along the same received subspace of *Eve*, i.e., the set of precoding matrix pairs that meet the requirements of the proposed scheme can be expressed as follows:

$$\bar{\mathcal{I}} = \{(\mathbf{V}_a, \mathbf{V}_b) | \text{span}(\mathbf{G}_a \mathbf{V}_a) = \text{span}(\mathbf{G}_b \mathbf{V}_b), (\mathbf{V}_a, \mathbf{V}_b) \in \mathcal{I}\}.$$

In this way, *Eve* can only see a distorted version of the message signal, and thus both R_e^a and R_e^b converge to a constant as P approaches infinity.

In order to solve the sum S.D.o.F. maximization problem, as in [24], we propose to align the signals from *Alice* and *Bob* along the same received subspace of *Eve*. However, due to the fact that *Eve* has interest in both source signals, it does not require the total signal streams the legitimate receiver can see to be no greater than the total number of receive antennas, and thus we get a new transmission scheme. Based on their potential to achieve a greater sum S.D.o.F., in the next section we will reclassify the candidate precoding vector pairs into eight subsets, determine the number of linearly independent candidate precoding vector pairs in each subset, and give their rankings in the construction of the precoding matrix pair. It turns out that the proposed scheme is sufficient to achieve the maximum sum S.D.o.F.. Details are given by the following proposition.

Proposition 1: Let

$$\bar{d}_s^{\text{sum}} \triangleq \max_{(\mathbf{V}_a, \mathbf{V}_b) \in \bar{\mathcal{I}}} (d_s^a + d_s^b). \quad (8)$$

Then $d_s^{\text{sum}} = \bar{d}_s^{\text{sum}}$.

Proof: See Appendix B. ■

By *Proposition 1*, we preclude a large number of precoding matrices, which have no contribution to the maximum achievable value of the sum S.D.o.F., and thus reduce the number of precoding matrices we need to investigate. In the sequel, we give *Corollary 1*, by which we further reduce the candidate precoding matrices.

Corollary 1: Let

$$\hat{d}_s^{\text{sum}} \triangleq \max_{(\mathbf{V}_a, \mathbf{V}_b) \in \hat{\mathcal{I}}} (d_s^a + d_s^b), \quad (9)$$

with $\hat{\mathcal{I}} = \{(\mathbf{V}_a, \mathbf{V}_b) | \mathbf{G}_a \mathbf{V}_a = \mathbf{G}_b \mathbf{V}_b, (\mathbf{V}_a, \mathbf{V}_b) \in \bar{\mathcal{I}}\}$. Then, $\bar{d}_s^{\text{sum}} = \bar{d}_s^{\text{sum}}$.

Proof: See Appendix C. ■

IV. FEASIBLE SET OF PRECODING VECTOR PAIRS OF THE PROPOSED SCHEME

The combination of *Proposition 1* and *Corollary 1* indicates that for the purpose of obtaining the maximum sum S.D.o.F., we only need to investigate the maximum achievable sum S.D.o.F. over the set of precoding matrix pairs $\hat{\mathcal{I}}$. Let $(\mathbf{v}_a, \mathbf{v}_b)$ be the precoding vectors comprising $(\mathbf{V}_a, \mathbf{V}_b) \in \hat{\mathcal{I}}$ (see the definition of $\hat{\mathcal{I}}$ under equation (9)). In this section, we construct $(\mathbf{V}_a, \mathbf{V}_b)$ one vector pair $(\mathbf{v}_a, \mathbf{v}_b)$ at a time.

Some observations are in order. First, obviously we are interested in linearly independent precoding vectors. Second, one can see that when the message signal sent by one source falls into the null space of the eavesdropping channel, the interference from the other source cannot degrade any further the eavesdropping channel because *Eve* already receives nothing; in those cases we may take the precoding vector at the other source to be zero. Third, for any precoding matrix pairs $(\mathbf{V}_a, \mathbf{V}_b) \in \hat{\mathcal{I}}$, since $\mathbf{G}_a \mathbf{V}_a = \mathbf{G}_b \mathbf{V}_b$, it holds that $n_1(\mathbf{V}_a, \mathbf{V}_b) = n_2(\mathbf{V}_a, \mathbf{V}_b) = 0$, which combined with *Lemma 1*, indicates

$$d_s^a = \dim\{\text{span}(\mathbf{H}_{ba} \mathbf{V}_a) \setminus \text{span}(\mathbf{H}_{bb} \mathbf{V}_b)\}, \quad (10a)$$

$$d_s^b = \dim\{\text{span}(\mathbf{H}_{ab} \mathbf{V}_b) \setminus \text{span}(\mathbf{H}_{aa} \mathbf{V}_a)\}. \quad (10b)$$

Thus, the sum of d_s^a and d_s^b increases as we include more linearly independent interference free precoding vector pairs in $(\mathbf{V}_a, \mathbf{V}_b)$. Fourth, since all the channel matrices are assumed to be full rank, and via (10a), (10b) one can see that

$$d_s^a = \min\{(N_b^r - \text{rank}\{\mathbf{H}_{bb} \mathbf{V}_b\})^+, \text{rank}\{\mathbf{H}_{ba} \mathbf{V}_a\}\}, \quad (11a)$$

$$d_s^b = \min\{(N_a^r - \text{rank}\{\mathbf{H}_{aa} \mathbf{V}_a\})^+, \text{rank}\{\mathbf{H}_{ab} \mathbf{V}_b\}\}, \quad (11b)$$

where the first term in the min operator denotes the dimension of the interference free subspace *Bob* and *Alice* can see, respectively; the second term in the min operator represents the number of message signal streams *Bob* and *Alice* can see, respectively. Motivated by these observations, we next divide the set of precoding vector pairs into eight subsets, namely, $Sub_{11}, \dots, Sub_{14}, Sub_{21}, \dots, Sub_{24}$.

Sub_{1i}: Either \mathbf{v}_a or \mathbf{v}_b falls into the null space of the eavesdropping channel. For the pairs in $Sub_{11} \cup Sub_{12}$ it holds that $\mathbf{v}_b = \mathbf{0}$; for the pairs in $Sub_{13} \cup Sub_{14}$ it holds that $\mathbf{v}_a = \mathbf{0}$. *Alice* is self-interference free and suffers from self-interference for the pairs in $Sub_{11} \cup Sub_{12}$, respectively. *Bob* is self-interference free and suffers from self-interference for the pairs in $Sub_{13} \cup Sub_{14}$, respectively.

Sub_{2i}: Both \mathbf{v}_a and \mathbf{v}_b do not lie within the null space of the eavesdropping channel. For the pairs in Sub_{21} , both *Alice* and *Bob* are self-interference free; for the pairs in Sub_{22} , *Bob* is self-interference free, but *Alice* suffers from self-interference; for the pairs in Sub_{23} , *Alice* is self-interference free, but *Bob* suffers from self-interference; for the pairs in Sub_{24} , both *Alice* and *Bob* suffer from self-interference.

In the sequel, we will first derive the formula for \mathbf{v}_a and \mathbf{v}_b in each subset. As it will become clear, the formula for

$(\mathbf{v}_a, \mathbf{v}_b)$ in different subsets may have some common basis vectors; in those cases, and since we are interested in linearly independent \mathbf{v}_a 's and \mathbf{v}_b 's, the common basis vectors will only be attributed to the subset with the highest priority, i.e., its precoding vector pairs have the potential to achieve a greater sum of d_s^a and d_s^b . Based on these observations, we then determine the number of linearly independent candidate precoding vector pairs in $Sub_{11}, \dots, Sub_{14}, Sub_{21}, \dots, Sub_{24}$, i.e., $d_{11}, \dots, d_{14}, d_{21}, \dots, d_{24}$, respectively.

A. The formulas for \mathbf{v}_a and \mathbf{v}_b in each subset

1) *Sub₁₁*: The precoding vectors in Sub_{11} should satisfy

$$\mathbf{G}_a \mathbf{v}_a = \mathbf{0}, \quad (12a)$$

$$\mathbf{H}_{aa} \mathbf{v}_a = \mathbf{0}. \quad (12b)$$

By definition, it holds that $\mathbf{G}_a \mathbf{v}_a = \mathbf{G}_b \mathbf{v}_b = \mathbf{0}$. In this subset we will only consider $\mathbf{v}_b = \mathbf{0}$, since even if $\mathbf{v}_b \neq \mathbf{0}$ the interference from *Bob* cannot degrade any further the eavesdropping channel.

Substituting $\mathbf{v}_a = \Gamma(\mathbf{G}_a) \mathbf{x}$ into (12b), with \mathbf{x} being an arbitrary vector with appropriate length, we arrive at $\mathbf{H}_{aa} \Gamma(\mathbf{G}_a) \mathbf{x} = \mathbf{0}$. This is equivalent to $\mathbf{x} = \Gamma(\mathbf{H}_{aa} \Gamma(\mathbf{G}_a)) \mathbf{y}$, with \mathbf{y} being an arbitrary vector with appropriate length.

Thus, the formula of \mathbf{v}_a in Sub_{11} is

$$\mathbf{v}_a = \Gamma(\mathbf{G}_a) \Gamma(\mathbf{H}_{aa} \Gamma(\mathbf{G}_a)) \mathbf{z}, \quad (13)$$

with \mathbf{z} being any nonzero vectors with appropriate length.

2) *Sub₁₂*: The precoding vectors in Sub_{12} should satisfy

$$\mathbf{G}_a \mathbf{v}_a = \mathbf{0}, \quad (14a)$$

$$\mathbf{H}_{aa} \mathbf{v}_a \neq \mathbf{0}. \quad (14b)$$

The vectors \mathbf{v}_a satisfying (14a) are of the form $\Gamma(\mathbf{G}_a) \mathbf{x}$. Because \mathbf{H}_{aa} is independent of \mathbf{G}_a , for precoding vectors satisfying (14a), $\mathbf{H}_{aa} \mathbf{v}_a \neq \mathbf{0}$ holds true with probability one. So, the vectors \mathbf{v}_a in Sub_{12} are of the form $\Gamma(\mathbf{G}_a) \mathbf{x}$.

On the other hand, since we want linearly independent precoding vectors, the beamforming direction already considered in the set with higher priority, e.g., Sub_{11} , should not be under consideration. Thus, in Sub_{12} we only consider the following vectors,

$$\mathbf{v}_a = \Gamma(\mathbf{G}_a) \Gamma^\perp(\mathbf{H}_{aa} \Gamma(\mathbf{G}_a)) \mathbf{z}. \quad (15)$$

3) *Sub₁₃*: The precoding vectors in Sub_{13} should satisfy

$$\mathbf{G}_b \mathbf{v}_b = \mathbf{0}, \quad (16a)$$

$$\mathbf{H}_{bb} \mathbf{v}_b = \mathbf{0}. \quad (16b)$$

In a similar way we derive the formula of \mathbf{v}_a in Sub_{11} , we obtain the formula of \mathbf{v}_b in Sub_{13} , i.e.,

$$\mathbf{v}_b = \Gamma(\mathbf{G}_b) \Gamma(\mathbf{H}_{bb} \Gamma(\mathbf{G}_b)) \mathbf{z}. \quad (17)$$

4) *Sub₁₄*: The precoding vectors in Sub_{14} should satisfy

$$\mathbf{G}_b \mathbf{v}_b = \mathbf{0}, \quad (18a)$$

$$\mathbf{H}_{bb} \mathbf{v}_b \neq \mathbf{0}. \quad (18b)$$

In a similar way we derive the formula of \mathbf{v}_a in Sub_{12} , we obtain the formula of \mathbf{v}_b in Sub_{14} , i.e.,

$$\mathbf{v}_b = \Gamma(\mathbf{G}_b)\Gamma^\perp(\mathbf{H}_{bb}\Gamma(\mathbf{G}_b))\mathbf{z}. \quad (19)$$

5) Sub_{21} : The precoding vector pairs in Sub_{21} should satisfy

$$\mathbf{H}_{bb}\mathbf{v}_b = \mathbf{0}, \quad (20a)$$

$$\mathbf{H}_{aa}\mathbf{v}_a = \mathbf{0}, \quad (20b)$$

$$\mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}. \quad (20c)$$

Substituting $\mathbf{v}_a = \Gamma(\mathbf{H}_{aa})\mathbf{x}$ and $\mathbf{v}_b = \Gamma(\mathbf{H}_{bb})\mathbf{y}$ into (20c) yields

$$\mathbf{G}_a\Gamma(\mathbf{H}_{aa})\mathbf{x} = \mathbf{G}_b\Gamma(\mathbf{H}_{bb})\mathbf{y} \neq \mathbf{0}. \quad (21)$$

Via *Proposition 1(i)* of [24] we arrive at \mathbf{x} and \mathbf{y} satisfying (21), i.e.,

$$\mathbf{x} = \hat{\Psi}_{12}\hat{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))\mathbf{z}_a,$$

$$\mathbf{y} = \hat{\Psi}_{22}\hat{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))\mathbf{z}_b,$$

where \mathbf{z}_a and \mathbf{z}_b denote any vectors with appropriate length; $\hat{\Psi}_{12}$, $\hat{\Lambda}_1$, $\hat{\Psi}_{22}$, $\hat{\Lambda}_2$, and \hat{s} (to be used in the next subsection) correspond to the Ψ_{12} , Λ_1 , Ψ_{22} , Λ_2 and s , and arise due to the GSVD of $(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))^H$ and $(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))^H$.

Thus, the formulas for \mathbf{v}_a and \mathbf{v}_b in Sub_{21} are of the form

$$\mathbf{v}_a = \Gamma(\mathbf{H}_{aa})\hat{\Psi}_{12}\hat{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{H}_{aa})\Gamma(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))\mathbf{z}_a, \quad (22a)$$

$$\mathbf{v}_b = \Gamma(\mathbf{H}_{bb})\hat{\Psi}_{22}\hat{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{H}_{bb})\Gamma(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))\mathbf{z}_b. \quad (22b)$$

6) Sub_{22} : The precoding vector pairs in Sub_{22} should satisfy

$$\mathbf{H}_{bb}\mathbf{v}_b = \mathbf{0}, \quad (23a)$$

$$\mathbf{H}_{aa}\mathbf{v}_a \neq \mathbf{0}, \quad (23b)$$

$$\mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}. \quad (23c)$$

Substituting $\mathbf{v}_b = \Gamma(\mathbf{H}_{bb})\mathbf{y}$ into (23c), we arrive at

$$\mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\Gamma(\mathbf{H}_{bb})\mathbf{y} \neq \mathbf{0}. \quad (24)$$

Via *Proposition 1(i)* of [24] we arrive at \mathbf{v}_a and \mathbf{y} satisfying (24), i.e.,

$$\mathbf{v}_a = \bar{\Psi}_{12}\bar{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{G}_a)\mathbf{z}_a,$$

$$\mathbf{y} = \bar{\Psi}_{22}\bar{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))\mathbf{z}_b,$$

where $\bar{\Psi}_{12}$, $\bar{\Lambda}_1$, $\bar{\Psi}_{22}$, $\bar{\Lambda}_2$, and \bar{s} (to be used in the next subsection) correspond to the Ψ_{12} , Λ_1 , Ψ_{22} , Λ_2 and s , and arise due to the GSVD of \mathbf{G}_a^H and $(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))^H$.

Thus, the formulas for \mathbf{v}_a and \mathbf{v}_b in Sub_{22} are of the form

$$\mathbf{v}_a = \bar{\Psi}_{12}\bar{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{G}_a)\mathbf{z}_a, \quad (25a)$$

$$\mathbf{v}_b = \Gamma(\mathbf{H}_{bb})\bar{\Psi}_{22}\bar{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{H}_{bb})\Gamma(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))\mathbf{z}_b. \quad (25b)$$

In the above, we used the fact that since \mathbf{H}_{aa} is independent of \mathbf{H}_{bb} , \mathbf{G}_a and \mathbf{G}_b , for the precoding vector pairs in (25a) and (25b), $\mathbf{H}_{aa}\mathbf{v}_a \neq \mathbf{0}$ holds true with probability one.

7) Sub_{23} : The precoding vector pairs in Sub_{23} should satisfy

$$\mathbf{H}_{bb}\mathbf{v}_b \neq \mathbf{0}, \quad (26a)$$

$$\mathbf{H}_{aa}\mathbf{v}_a = \mathbf{0}, \quad (26b)$$

$$\mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}. \quad (26c)$$

Substituting $\mathbf{v}_a = \Gamma(\mathbf{H}_{aa})\mathbf{x}$ into (26c), we arrive at

$$\mathbf{G}_a\Gamma(\mathbf{H}_{aa})\mathbf{x} = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}. \quad (27)$$

Via *Proposition 1(i)* of [24] we arrive at \mathbf{x} and \mathbf{v}_b satisfying (27), i.e.,

$$\mathbf{x} = \check{\Psi}_{12}\check{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))\mathbf{z}_a,$$

$$\mathbf{v}_b = \check{\Psi}_{22}\check{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{G}_b)\mathbf{z}_b.$$

where $\check{\Psi}_{12}$, $\check{\Lambda}_1$, $\check{\Psi}_{22}$, $\check{\Lambda}_2$, and \check{s} (to be used in the next subsection) correspond to the Ψ_{12} , Λ_1 , Ψ_{22} , Λ_2 and s , and arise due to the GSVD of $(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))^H$ and \mathbf{G}_b^H .

Thus, the formulas for \mathbf{v}_a and \mathbf{v}_b in Sub_{23} are of the form

$$\mathbf{v}_a = \Gamma(\mathbf{H}_{aa})\check{\Psi}_{12}\check{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{H}_{aa})\Gamma(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))\mathbf{z}_a, \quad (28a)$$

$$\mathbf{v}_b = \check{\Psi}_{22}\check{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{G}_b)\mathbf{z}_b. \quad (28b)$$

8) Sub_{24} : The precoding vector pairs in Sub_{24} should satisfy

$$\mathbf{H}_{bb}\mathbf{v}_b \neq \mathbf{0}, \quad (29a)$$

$$\mathbf{H}_{aa}\mathbf{v}_a \neq \mathbf{0}, \quad (29b)$$

$$\mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}. \quad (29c)$$

Via *Proposition 1(i)* of [24] we arrive at that the formulas for \mathbf{v}_a and \mathbf{v}_b in Sub_{24} are of the form

$$\mathbf{v}_a = \tilde{\Psi}_{12}\tilde{\Lambda}_1^{-1}\mathbf{z} + \Gamma(\mathbf{G}_a)\mathbf{z}_a, \quad (30a)$$

$$\mathbf{v}_b = \tilde{\Psi}_{22}\tilde{\Lambda}_2^{-1}\mathbf{z} + \Gamma(\mathbf{G}_b)\mathbf{z}_b, \quad (30b)$$

where $\tilde{\Psi}_{12}$, $\tilde{\Lambda}_1$, $\tilde{\Psi}_{22}$, $\tilde{\Lambda}_2$, and \tilde{s} (to be used in the next subsection) correspond to the Ψ_{12} , Λ_1 , Ψ_{22} , Λ_2 and s , and arise due to the GSVD of \mathbf{G}_a^H and \mathbf{G}_b^H .

B. The number of linearly independent candidate precoding vector pairs in each subset

Since all the channel matrices are assumed to be full rank, and by (13)(15)(17)(19), it respectively holds that

$$d_{11} \leq (N_a^t - N_e - N_a^r)^+, \quad (31a)$$

$$d_{12} \leq \min\{N_a^r, (N_a^t - N_e)^+\}, \quad (31b)$$

$$d_{13} \leq (N_b^t - N_e - N_b^r)^+, \quad (31c)$$

$$d_{14} \leq \min\{N_b^r, (N_b^t - N_e)^+\}. \quad (31d)$$

From the above subsection, one can see that the formulas for \mathbf{v}_a and \mathbf{v}_b in Sub_{1i} , $i = 1, \dots, 4$, may have some common basis vectors with those in Sub_{2j} , $j = 1, \dots, 4$. For example, some basis vectors of \mathbf{v}_a in Sub_{21} , i.e., $\Gamma(\mathbf{H}_{aa})\Gamma(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))$, also span the solution space of Sub_{11} , since they span the same space as $\Gamma(\mathbf{G}_a)\Gamma(\mathbf{H}_{aa}\Gamma(\mathbf{G}_a))$; some basis vectors of \mathbf{v}_b in Sub_{21} , i.e., $\Gamma(\mathbf{H}_{bb})\Gamma(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))$, also span the solution space of Sub_{13} , since they span the same space as $\Gamma(\mathbf{G}_b)\Gamma(\mathbf{H}_{bb}\Gamma(\mathbf{G}_b))$. Since we are interested in linearly

TABLE I: The maximum number of linearly independent candidate precoding vector pairs.

Subsets	Maximum number of linearly independent vectors
Sub_{11}	$d_{11} = (N_a^t - N_e - N_a^r)^+$
Sub_{12}	$d_{12} = \min\{N_a^r, (N_a^t - N_e)^+\}$
Sub_{13}	$d_{13} = (N_b^t - N_e - N_b^r)^+$
Sub_{14}	$d_{14} = \min\{N_b^r, (N_b^t - N_e)^+\}$
Sub_{21}	$d_{21} = \hat{s}$
Sub_{22}	$d_{22} = \bar{s} - d_{21}$
Sub_{23}	$d_{23} = \check{s} - d_{21}$
Sub_{24}	$d_{24} = \bar{s} - (d_{21} + d_{22} + d_{23})$

independent \mathbf{v}_a 's and \mathbf{v}_b 's, the number of linearly independent precoding vectors \mathbf{v}_a and \mathbf{v}_b considered in Sub_{21} should be equal. Moreover, any paired selection of those basis vectors from Sub_{21} cannot help increase the sum S.D.o.F., as compared with the case in which we respectively attribute those basis vectors to Sub_{11} and Sub_{13} . Thus, for the pairs in Sub_{21} , we do not consider the basis vectors $\Gamma(\mathbf{H}_{aa})\Gamma(\mathbf{G}_a\Gamma(\mathbf{H}_{aa}))$ and $\Gamma(\mathbf{H}_{bb})\Gamma(\mathbf{G}_b\Gamma(\mathbf{H}_{bb}))$. Therefore,

$$d_{21} \leq \hat{s}. \quad (32)$$

The above arguments also apply to Sub_{22} , Sub_{23} and Sub_{24} . Thus, the equalities in (31a)-(31d) hold true.

On the other hand, on combining (20a)-(20c) with (23a)-(23c), it holds that

$$Sub_{21} \cup Sub_{22} = \{(\mathbf{v}_a, \mathbf{v}_b) | \mathbf{H}_{bb}\mathbf{v}_b = \mathbf{0}, \mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}\}.$$

Thus,

$$d_{22} + d_{21} \leq \bar{s}. \quad (33)$$

On combining (20a)-(20c) with (26a)-(26c), it holds that

$$Sub_{21} \cup Sub_{23} = \{(\mathbf{v}_a, \mathbf{v}_b) | \mathbf{H}_{aa}\mathbf{v}_a = \mathbf{0}, \mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}\}.$$

Thus,

$$d_{23} + d_{21} \leq \check{s}. \quad (34)$$

On combining (20a)-(20c) with (23a)-(23c), (26a)-(26c) and (29a)-(29c), it holds that $Sub_{21} \cup Sub_{22} \cup Sub_{23} \cup Sub_{24} = \{(\mathbf{v}_a, \mathbf{v}_b) | \mathbf{G}_a\mathbf{v}_a = \mathbf{G}_b\mathbf{v}_b \neq \mathbf{0}\}$. Thus,

$$d_{24} + d_{23} + d_{22} + d_{21} \leq \bar{s}. \quad (35)$$

Regarding the priority of Sub_{2j} , $j = 1, \dots, 4$, Sub_{21} ranks the highest and Sub_{24} ranks the lowest. Therefore, all the inequalities in (32)-(35) hold true.

Based on the above discussions, and using (44d), Table I provides the number of linearly independent vectors $(\mathbf{v}_a, \mathbf{v}_b)$'s that should be considered in each subset.

V. CONSTRUCTION OF $(\mathbf{V}_a, \mathbf{V}_b)$ WHICH ACHIEVES THE MAXIMUM SUM S.D.o.F.

The key idea for achieving the maximum sum S.D.o.F. is to include as many interference free precoding vector pairs (interference free signal streams) in $(\mathbf{V}_a, \mathbf{V}_b)$ as possible. To

achieve that goal, in the construction of $(\mathbf{V}_a, \mathbf{V}_b)$, we will select as many precoding vector pairs $(\mathbf{v}_a, \mathbf{v}_b)$ from the subset with higher priority as possible. When there are no more available pairs in a given subset, we will consider the next subset in terms of priority.

By the definition of each subset and the equations in (11a) and (11b), one can see that Sub_{21} has the highest priority, followed by $Sub_{11} \cup Sub_{13} \cup Sub_{22} \cup Sub_{23}$, and then $Sub_{24} \cup Sub_{12} \cup Sub_{14}$, i.e.,

$$Sub_{21} \succ Sub_{11} \cup Sub_{13} \cup Sub_{22} \cup Sub_{23} \succ Sub_L, \quad (36)$$

where $Sub_L \triangleq Sub_{24} \cup Sub_{12} \cup Sub_{14}$. Moreover, Sub_{12} and Sub_{14} have the same priority. Sub_{24} has higher priority than $Sub_{12} \cup Sub_{14}$ except for the case in which the dimensions of the available interference free receive subspace *Alice* and *Bob* can see are both equal to one. The priorities of Sub_{11} , Sub_{13} , Sub_{22} and Sub_{23} depend on the number of antennas, and also the available interference free receive subspace *Alice* and *Bob* can respectively see.

In the following, we will consider four distinct cases, i.e., the case of $N_a^t \leq N_e + N_a^r$ and $N_b^t \leq N_e + N_b^r$, the case of $N_a^t \leq N_e + N_a^r$ and $N_b^t > N_e + N_b^r$, the case of $N_a^t > N_e + N_a^r$ and $N_b^t \leq N_e + N_b^r$, and the case of $N_a^t > N_e + N_a^r$ and $N_b^t > N_e + N_b^r$. For each case, we will determine the specific rankings of Sub_{11} , Sub_{13} , Sub_{22} and Sub_{23} .

By those rankings, we include precoding vector pairs into the precoding matrix pair $(\mathbf{V}_a, \mathbf{V}_b)$ one by one, until adding more precoding vector pairs does not increase the achievable sum S.D.o.F.. With this constructive method and stop criteria, we then determine the maximum achievable sum S.D.o.F..

A. $N_a^t \leq N_e + N_a^r$, $N_b^t \leq N_e + N_b^r$.

In this case, and based on Table I it holds that $d_{11} = d_{13} = 0$. Thus, we only need to consider the rankings of Sub_{22} and Sub_{23} . By definition, for the precoding vector pairs from Sub_{22} *Bob* is self-interference free while *Alice* suffers from self-interference; for the precoding vector pairs from Sub_{23} the situation reverses. Combined with (11a) and (11b), one can see that if *Alice* has a greater interference free receive subspace, Sub_{22} is of higher priority; otherwise, Sub_{23} is of higher priority. For example, consider the case $N_b^r = 1$ and $N_a^r = 2$, selecting one pair from Sub_{22} achieves a sum S.D.o.F. of 2, while selecting one pair from Sub_{23} can only achieve a sum S.D.o.F. of 1.

So far, we have obtained the specific rankings for all the subsets, based on which, we include precoding vector pairs into the precoding matrix pair $(\mathbf{V}_a, \mathbf{V}_b)$ one by one, until the further adding of precoding vector pairs could not help increase the achievable sum S.D.o.F.. This constructive method also provides us a way to determine the maximum achievable S.D.o.F.. In the following, we will consider two distinct subcases, i.e., the subcase of $N_b^r \geq N_a^r$ and the subcase of $N_b^r < N_a^r$.

i) For the subcase of $N_b^r \geq N_a^r$.

Following (36) and the rankings discussed above, we first pick pairs from Sub_{21} . Until there are no available pairs in Sub_{21} , we next consider pairs from Sub_{22} and Sub_{23} . Sub_{23}

$$\begin{aligned}
q_1 &= \min^+ \{\max\{N_b^r, N_a^r\}, d_{21}\}, \\
q_2 &= \min^+ \{\max\{\lfloor \frac{N_b^r - q_1}{2} \rfloor, N_a^r - q_1\}, \min\{N_b^r - N_a^r, d_{23}\}\}, \\
q_3 &= 2\min^+ \{\max\{\lfloor \frac{N_b^r - q_1 - 2q_2}{3} \rfloor, \lfloor \frac{N_a^r - q_1 - q_2}{3} \rfloor\}, \bar{d}_{23}\}, \\
q_4 &= \min^+ \{\max\{N_b^r - q_1 - 2q_2 - 3q_3, \lfloor \frac{N_a^r - q_1 - q_2 - 3q_3}{2} \rfloor\}, d_{22} - q_3\}, \\
q_5 &= \min^+ \{\max\{\lfloor \frac{N_b^r - q_1 - 2q_2 - 3q_3 - q_4}{2} \rfloor, \lfloor \frac{N_a^r - q_1 - q_2 - 3q_3 - 2q_4}{2} \rfloor\}, d_{24}\}, \\
q_6 &= \min^+ \{\min\{N_b^r - q_1 - 2q_2 - 3q_3 - q_4 - 2q_5, N_a^r - q_1 - q_2 - 3q_3 - 2q_4 - 2q_5\}, d_{12}\}, \\
q_7 &= \min^+ \{\min\{N_b^r - q_1 - 2q_2 - 3q_3 - q_4 - 2q_5 - q_6, N_a^r - q_1 - q_2 - 3q_3 - 2q_4 - 2q_5 - q_6\}, d_{14}\}.
\end{aligned} \tag{37}$$

has higher priority and its pairs are at the first consideration, since *Bob* can see a bigger interference free receive subspace. However, as we include one pair from *Sub*₂₃, the dimension of the available interference free receive subspace *Bob* and *Alice* respectively decreases by two and one. After selecting $N_b^r - N_a^r + 1$ pairs from *Sub*₂₃, *Alice* has a greater interference free receive subspace, which indicates that *Sub*₂₂ has higher priority. Similarly, as we include one pair from *Sub*₂₂, the dimension of the available interference free receive subspace that *Alice* and *Bob* can see respectively decreases by one and two. Thus, following the selection of one pair from *Sub*₂₃, the pairs from *Sub*₂₂ have higher priority. Summarizing the above observations, after picking all the pairs from *Sub*₂₁, we will first select $\min\{d_{23}, N_b^r - N_a^r\}$ pairs from *Sub*₂₃; we then select pairs from *Sub*₂₂ and *Sub*₂₃ in turn, one by one, until there are no more available pairs in *Sub*₂₂ or *Sub*₂₃. Subsequently, we select pairs from the remaining pairs from *Sub*₂₂ or *Sub*₂₃, followed by *Sub*_L.

Based on the above constructive method, we now can determine the maximum achievable S.D.o.F. Divide *Sub*₂₃ into two subsets, i.e., *Sub*₂₃¹ and *Sub*₂₃², with a number of $\min\{d_{23}, N_b^r - N_a^r\}$ and $\bar{d}_{23} \triangleq d_{23} - \min\{d_{23}, N_b^r - N_a^r\}$ precoding vector pairs, respectively. Assume that $d_{22} \geq \bar{d}_{23}$. Then, we will first run out of pairs of *Sub*₂₃². Therefore, in the construction of $(\mathbf{V}_a, \mathbf{V}_b)$, the subsets are ranked as

$$Sub_{21} \succ Sub_{23}^1 \succ \{Sub_{22}, Sub_{23}^2\} \succ Sub_{22} \succ Sub_L,$$

where by $\{Sub_{22}, Sub_{23}^2\}$ we mean that we select pairs from *Sub*₂₂ and *Sub*₂₃ in turn. Let $q_1, q_2, q_3, q_4, q_5, q_6$ and q_7 be the number of precoding vector pairs we pick from *Sub*₂₁, *Sub*₂₃¹, $\{Sub_{22}, Sub_{23}^2\}$, *Sub*₂₂, *Sub*₂₄, *Sub*₁₂ and *Sub*₁₄, respectively. Since we stop picking until the further adding of precoding vector pairs could not help increase the achievable sum S.D.o.F., the expressions of $q_1, q_2, q_3, q_4, q_5, q_6$ and q_7 can be written as in (37) at the top of this page.

According to (11a), the achieved S.D.o.F. of the *Alice-Bob* channel is

$$d_1^a = \min\{(N_b^r - q_2 - \frac{q_3}{2} - q_5 - q_7)^+, \sum_{i=1}^6 q_i\}.$$

According to (11b), the achieved S.D.o.F. of the *Bob-Alice*

channel is

$$d_1^b = \min\{(N_a^r - q_2 - \frac{q_3}{2} - q_4 - q_5 - q_6)^+, (\sum_{i=1}^7 q_i) - q_6\}.$$

Therefore, the maximum achievable sum S.D.o.F. is

$$d_s^{\text{sum}} = d_1^b + d_1^a. \tag{38}$$

Example 1: Consider the case $(N_a^t, N_b^t) = (5, 2)$, $(N_b^t, N_b^r) = (4, 3)$ and $N_e = 5$. Based on Table I, the maximum number of linearly independent precoding vector pairs in each subset is $d_{11} = d_{12} = d_{13} = d_{14} = d_{21} = 0$, $d_{22} = 1$, $d_{23} = 2$, $d_{24} = 1$. Since $N_b^r \geq N_a^r$, we divide *Sub*₂₃ into two subsets, i.e., *Sub*₂₃¹ and *Sub*₂₃², with each consisting of one precoding vector pair. By the rankings derived above, i.e., $Sub_{23}^1 \succ \{Sub_{22}, Sub_{23}^2\} \succ Sub_{22} \succ Sub_{24}$, we first select a precoding vector pair from *Sub*₂₃¹, i.e., $(\mathbf{v}_a^1, \mathbf{v}_b^1)$. The dimension of the remaining available interference free receive subspace of *Alice* and *Bob* are $N_a^r - 2 = 1$ and $N_b^r - 1 = 1$, respectively. For the remaining precoding vector pairs, we stop selecting after we take one more from *Sub*₂₂, i.e., $(\mathbf{v}_a^2, \mathbf{v}_b^2)$, since additional precoding vector pairs will introduce extra CCI without increasing the sum S.D.o.F. For *Sub*₂₃¹, it holds that $\mathbf{H}_{aa}\mathbf{v}_a^1 = \mathbf{0}$. for *Sub*₂₂, it holds that $\mathbf{H}_{bb}\mathbf{v}_b^2 = \mathbf{0}$. Therefore, for $\mathbf{V}_a = [\mathbf{v}_a^1, \mathbf{v}_a^2]$ and $\mathbf{V}_b = [\mathbf{v}_b^1, \mathbf{v}_b^2]$, with (11a) and (11b) it holds that $d_s^a = 1$ and $d_s^b = 2$. Concluding, a sum S.D.o.F. of 3 can be achieved.

The precoding vector pair selection procedure for the case of $d_{22} \leq \bar{d}_{23}$ is similar to that for the case of $d_{22} > \bar{d}_{23}$. Moreover, the maximum achievable sum S.D.o.F. can be obtained by (38), with the place of \bar{d}_{23} and d_{22} in (37) exchanged.

ii) The discussion for the subcase of $N_b^r < N_a^r$ is omitted since it is similar to that for the subcase of $N_b^r \geq N_a^r$.

B. $N_a^t \leq N_e + N_a^r, N_b^t > N_e + N_b^r$.

In this case, and based on Table I it holds that $d_{11} = d_{23} = d_{24} = 0$. Thus, we only need to consider the rankings of *Sub*₁₃ and *Sub*₂₂. By definition, for the precoding vector pairs from *Sub*₁₃, $\mathbf{v}_a = \mathbf{0}$ and *Bob* is self-interference free; for the precoding vector pairs from *Sub*₂₂, *Bob* is self-interference free while *Alice* suffers from self-interference. Combined with (11a) and (11b), one can see that *Sub*₂₂ has higher priority than *Sub*₁₃ except for the case in which the

dimension of the available interference free receive subspace *Bob* can see is zero. Divide Sub_{22} into two subsets, i.e., Sub_{22}^1 and Sub_{22}^2 , with a number of $\min\{d_{22}, N_b^r\}$ and $\hat{d}_{22} \triangleq d_{22} - \min\{d_{22}, N_b^r\}$ precoding vector pairs, respectively. Based on what discussed above, we consider the following rankings:

$$Sub_{21} \succ Sub_{22}^1 \succ Sub_{13} \succ Sub_{22}^2 \succ Sub_{12} = Sub_{14}.$$

Let $\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_5$ and ζ_6 be the number of precoding vector pairs we pick from $Sub_{21}, Sub_{22}^1, Sub_{13}, Sub_{22}^2, Sub_{12}$ and Sub_{14} , respectively. We stop picking until the further adding of precoding vector pairs could not help increase the achievable sum S.D.o.F. Then, the expressions of $\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_5$ and ζ_6 are as follows:

$$\begin{aligned} \zeta_1 &= \min^+\{\max\{N_b^r, N_a^r\}, d_{21}\}, \\ \zeta_2 &= \min^+\{\max\{N_b^r - \zeta_1, \lfloor \frac{N_a^r - \zeta_1}{2} \rfloor\}, \min\{d_{22}, N_b^r\}\}, \\ \zeta_3 &= \min^+\{N_a^r - \zeta_1 - 2\zeta_2, d_{13}\}, \\ \zeta_4 &= \min^+\{\max\{N_b^r - \zeta_1 - \zeta_2, \lfloor \frac{N_a^r - \zeta_1 - 2\zeta_2 - \zeta_3}{2} \rfloor\}, \hat{d}_{22}\}, \\ \zeta_5 &= \min^+\{\min\{N_b^r - \zeta_1 - \zeta_2 - \zeta_4, \bar{N}_a^r\}, d_{12}\}, \\ \zeta_6 &= \min^+\{\min\{N_b^r - \zeta_1 - \zeta_2 - \zeta_4 - \zeta_5, \bar{N}_a^r - \zeta_5\}, d_{14}\}, \end{aligned}$$

with $\bar{N}_a^r = N_a^r - \zeta_1 - 2\zeta_2 - \zeta_3 - 2\zeta_4$.

According to (11a), the achieved S.D.o.F. of the *Alice-Bob* channel is

$$d_{II}^a = \min\{(N_b^r - \zeta_6)^+, \zeta_1 + \zeta_2 + \zeta_4 + \zeta_5\},$$

According to (11b), the achieved S.D.o.F. of the *Bob-Alice* channel is

$$d_{II}^b = \min\{(N_a^r - \zeta_2 - \zeta_4 - \zeta_5)^+, \zeta_1 + \zeta_2 + \zeta_3 + \zeta_4 + \zeta_6\}.$$

Therefore, the maximum achievable sum S.D.o.F. is

$$d_s^{\text{sum}} = d_{II}^b + d_{II}^a. \quad (39)$$

Example 2: Consider the case $(N_a^t, N_a^r) = (4, 6)$, $(N_b^t, N_b^r) = (8, 2)$ and $N_e = 5$. Based on Table I, the number of candidate precoding vector pairs in each subset is $d_{11} = d_{12} = d_{21} = d_{23} = d_{24} = 0$, $d_{13} = 1$, $d_{14} = 2$, $d_{22} = 4$. Since $Sub_{22}^1 \succ Sub_{13} \succ Sub_{22}^2 \succ Sub_{14}$, the precoding vector pairs of Sub_{22}^1 are at the first consideration. Thus, we first select two precoding vector pairs from Sub_{22}^1 , i.e., $(\mathbf{v}_a^1, \mathbf{v}_b^1)$ and $(\mathbf{v}_a^2, \mathbf{v}_b^2)$. The dimension of the remaining available interference free receive subspace of *Alice* and *Bob* are $N_a^r - 4 = 2$ and $N_b^r - 2 = 0$, respectively. For the remaining pairs, we stop after we take one more from Sub_{13} , i.e., $(\mathbf{v}_a^3, \mathbf{v}_b^3)$, since additional precoding vector will introduce extra CCI without increasing the sum S.D.o.F. For Sub_{22}^2 , it holds that $\mathbf{H}_{bb}\mathbf{v}_b^1 = \mathbf{0}$ and $\mathbf{H}_{bb}\mathbf{v}_b^2 = \mathbf{0}$; for Sub_{13} , it holds that $\mathbf{H}_{bb}\mathbf{v}_b^3 = \mathbf{0}$. Therefore, for $\mathbf{V}_a = [\mathbf{v}_a^1, \mathbf{v}_a^2, \mathbf{v}_a^3]$ and $\mathbf{V}_b = [\mathbf{v}_b^1, \mathbf{v}_b^2, \mathbf{v}_b^3]$, with (11a) and (11b) it holds that $d_s^a = 2$ and $d_s^b = 3$. Concluding, a sum S.D.o.F. of 5 can be achieved.

C. $N_a^t > N_e + N_a^r$, $N_b^t \leq N_e + N_b^r$.

In this case, and based on Table I it holds that $d_{13} = d_{22} = d_{24} = 0$. Thus, we only need to consider the rankings of Sub_{11} and Sub_{23} . By definition, for the precoding vector pairs from

Sub_{11} , $\mathbf{v}_b = \mathbf{0}$ and *Alice* is self-interference free; for the precoding vector pairs from Sub_{23} , *Alice* is self-interference free while *Bob* suffers from self-interference. Combined with (11a) and (11b), one can see that Sub_{23} has higher priority than Sub_{11} except for the case in which the dimension of the available interference free receive subspace *Alice* can see is zero. Divide Sub_{23} into two subsets, i.e., Sub_{23}^1 and Sub_{23}^2 , with a number of $\min\{d_{23}, N_a^r\}$ and $\hat{d}_{23} \triangleq d_{23} - \min\{d_{23}, N_a^r\}$ precoding vector pairs, respectively. Based on what discussed above, we consider the following rankings:

$$Sub_{21} \succ Sub_{23}^1 \succ Sub_{11} \succ Sub_{23}^2 \succ Sub_{12} = Sub_{14}.$$

Let $\eta_1, \eta_2, \eta_3, \eta_4, \eta_5$ and η_6 be the number of precoding vector pairs we pick from $Sub_{21}, Sub_{23}^1, Sub_{11}, Sub_{23}^2, Sub_{12}$ and Sub_{14} , respectively. We stop picking until the further adding of precoding vector pairs could not help increase the achievable sum S.D.o.F. Then, the expressions of $\eta_1, \eta_2, \eta_3, \eta_4, \eta_5$ and η_6 are as follows:

$$\begin{aligned} \eta_1 &= \min^+\{\max\{N_a^r, N_b^r\}, d_{21}\}, \\ \eta_2 &= \min^+\{\max\{\lfloor \frac{N_b^r - \eta_1}{2} \rfloor, N_a^r - \eta_1\}, \min\{d_{23}, N_a^r\}\}, \\ \eta_3 &= \min^+\{N_b^r - \eta_1 - 2\eta_2, d_{11}\}, \\ \eta_4 &= \min^+\{\max\{\lfloor \frac{N_b^r - \eta_1 - 2\eta_2 - \eta_3}{2} \rfloor, N_a^r - \eta_1 - \eta_2\}, \hat{d}_{23}\}, \\ \eta_5 &= \min^+\{\min\{\bar{N}_b^r, N_a^r - \eta_1 - \eta_2 - \eta_4\}, d_{12}\}, \\ \eta_6 &= \min^+\{\min\{\bar{N}_b^r - \eta_5, N_a^r - \eta_1 - \eta_2 - \eta_4 - \eta_5\}, d_{14}\}, \end{aligned}$$

with $\bar{N}_b^r = N_b^r - \eta_1 - 2\eta_2 - \eta_3 - 2\eta_4$.

According to (11a), the achieved S.D.o.F. of the *Alice-Bob* channel is

$$d_{III}^a = \min\{(N_b^r - \eta_2 - \eta_4 - \eta_6)^+, \eta_1 + \eta_2 + \eta_3 + \eta_4 + \eta_5\}.$$

According to (11b), the achieved S.D.o.F. of the *Bob-Alice* channel is

$$d_{III}^b = \min\{(N_a^r - \eta_5)^+, \eta_1 + \eta_2 + \eta_4 + \eta_6\}.$$

Therefore, the maximum achievable sum S.D.o.F. is

$$d_s^{\text{sum}} = d_{III}^b + d_{III}^a. \quad (40)$$

D. $N_a^t > N_e + N_a^r$, $N_b^t > N_e + N_b^r$.

In this case, and based on Table I it holds that $d_{22} = d_{23} = d_{24} = 0$. Thus, we only need to consider the rankings of Sub_{11} and Sub_{13} . By definition, for the precoding vector pairs in Sub_{11} , $\mathbf{v}_b = \mathbf{0}$ and *Alice* is self-interference free; for the precoding vector pairs in Sub_{13} , $\mathbf{v}_a = \mathbf{0}$ and *Bob* is self-interference free. Therefore, the relative rankings of Sub_{11} and Sub_{13} will not affect the achievable sum S.D.o.F. In the construction of $(\mathbf{V}_a, \mathbf{V}_b)$, the subsets are ranked as

$$Sub_{21} \succ Sub_{11} = Sub_{13} \succ Sub_{12} = Sub_{14}.$$

Let t_1, t_2, t_3, t_4 and t_5 be the number of precoding vector pairs we pick from $Sub_{21}, Sub_{11}, Sub_{13}, Sub_{12}$ and Sub_{14} , respectively. We stop picking until the further adding of precoding vector pairs could not help increase the achievable

TABLE II: An algorithm for constructing $(\mathbf{V}_a, \mathbf{V}_b)$ which achieves the maximum sum S.D.o.F.

Step 1. Initialization: compute d_{ij} , $i = 1, 2$, $j = 1, \dots, 4$, according to Table I; compute the precoding vector pairs $(\mathbf{v}_a, \mathbf{v}_b)$ for Sub_{ij} , $i = 1, 2$, $j = 1, \dots, 4$, with (13)(15) (17)(19)(22a)(22b)(25a)(25b)(28a)(28b)(30a)(30b), respectively.

Step 2. Rankings for different number of antennas:

Case A: $N_a^t \leq N_e + N_a^r$ and $N_b^t \leq N_e + N_b^r$.

i) If $N_b^r \geq N_a^r$, divide Sub_{23} into Sub_{23}^1 and Sub_{23}^2 , with a number of $\min\{d_{23}, N_b^r - N_a^r\}$ and $\bar{d}_{23} \triangleq d_{23} - \min\{d_{23}, N_b^r - N_a^r\}$ precoding vector pairs, respectively.

a) If $d_{22} \geq \bar{d}_{23}$, the subsets are ranked as $Sub_{21} \succ Sub_{23}^1 \succ \{Sub_{22}, Sub_{23}^2\} \succ Sub_{22} \succ Sub_{24} \cup Sub_{12} \cup Sub_{14}$.

b) If $d_{22} < \bar{d}_{23}$, the subsets are ranked as $Sub_{21} \succ Sub_{23}^1 \succ \{Sub_{22}, Sub_{23}^2\} \succ Sub_{23}^2 \succ Sub_{24} \cup Sub_{12} \cup Sub_{14}$.

ii) If $N_b^r < N_a^r$, divide Sub_{22} into Sub_{22}^1 and Sub_{22}^2 , with a number of $\min\{d_{22}, N_a^r - N_b^r\}$ and $\bar{d}_{22} \triangleq d_{22} - \min\{d_{22}, N_a^r - N_b^r\}$ precoding vector pairs, respectively.

a) If $d_{23} \geq \bar{d}_{22}$, the subsets are ranked as $Sub_{21} \succ Sub_{22}^1 \succ \{Sub_{23}, Sub_{22}^2\} \succ Sub_{23} \succ Sub_{24} \cup Sub_{12} \cup Sub_{14}$.

b) If $d_{23} < \bar{d}_{22}$, the subsets are ranked as $Sub_{21} \succ Sub_{22}^1 \succ \{Sub_{23}, Sub_{22}^2\} \succ Sub_{22}^2 \succ Sub_{24} \cup Sub_{12} \cup Sub_{14}$.

Case B: $N_a^t \leq N_e + N_a^r$, $N_b^t > N_e + N_b^r$.

Divide Sub_{22} into two subsets, i.e., Sub_{22}^1 and Sub_{22}^2 , with a number of $\min\{d_{22}, N_b^r\}$ and $\hat{d}_{22} \triangleq d_{22} - \min\{d_{22}, N_b^r\}$ precoding vector pairs, respectively. The subsets are ranked as $Sub_{21} \succ Sub_{22}^1 \succ Sub_{13} \succ Sub_{22}^2 \succ Sub_{12} = Sub_{14}$.

Case C: $N_a^t > N_e + N_a^r$, $N_b^t \leq N_e + N_b^r$.

Divide Sub_{23} into two subsets, i.e., Sub_{23}^1 and Sub_{23}^2 , with a number of $\min\{d_{23}, N_a^r\}$ and $\hat{d}_{23} \triangleq d_{23} - \min\{d_{23}, N_a^r\}$ precoding vector pairs, respectively. The subsets are ranked as $Sub_{21} \succ Sub_{23}^1 \succ Sub_{11} \succ Sub_{23}^2 \succ Sub_{12} = Sub_{14}$.

Case D: $N_a^t > N_e + N_a^r$, $N_b^t > N_e + N_b^r$.

The subsets are ranked as $Sub_{21} \succ Sub_{11} = Sub_{13} \succ Sub_{12} = Sub_{14}$.

Step 3. Include precoding vector pairs into $(\mathbf{V}_a, \mathbf{V}_b)$ one by one from Sub_{ij} , $i = 1, 2$, $j = 1, \dots, 4$, according to the rankings listed in Step 2. Stop when adding more precoding vector pairs does increase the achievable sum S.D.o.F.

Step 4. Output: $(\mathbf{V}_a, \mathbf{V}_b)$.

sum S.D.o.F. Then, the expressions of t_1, t_2, t_3, t_4 and t_5 are as follows:

$$\begin{aligned} t_1 &= \min^+\{\max\{N_a^r, N_b^r\}, d_{21}\}, \\ t_2 &= \min^+\{N_b^r - t_1, d_{11}\}, \\ t_3 &= \min^+\{N_a^r - t_1, d_{13}\}, \\ t_4 &= \min^+\{\min\{N_b^r - t_1 - t_2, N_a^r - t_1 - t_3\}, d_{12}\}, \\ t_5 &= \min^+\{\min\{N_b^r - t_1 - t_2 - t_4, N_a^r - t_1 - t_3 - t_4\}, d_{14}\}. \end{aligned}$$

According to (11a), the achieved S.D.o.F. of the *Alice-Bob* channel is

$$d_{IV}^a = \min\{(N_b^r - t_5)^+, t_1 + t_2 + t_4\}.$$

According to (11b), the achieved S.D.o.F. of the *Bob-Alice* channel is

$$d_{IV}^b = \min\{(N_a^r - t_4)^+, t_1 + t_3 + t_5\}.$$

Therefore, the maximum achievable sum S.D.o.F. is

$$d_s^{\text{sum}} = d_{IV}^b + d_{IV}^a. \quad (41)$$

Example 3: Consider the case $(N_a^t, N_b^r) = (7, 4)$, $(N_b^t, N_a^r) = (7, 4)$ and $N_e = 2$. Based on Table I, the maximum number of linearly independent precoding vector pairs in each subset is $d_{11} = d_{13} = 1$, $d_{12} = d_{14} = 4$, $d_{21} = 2$, $d_{22} = d_{23} = d_{24} = 0$. By the rankings $Sub_{21} \succ Sub_{11} = Sub_{13} \succ Sub_{12} = Sub_{14}$, we first select two precoding vector pairs from Sub_{21} , one precoding vector pair from Sub_{11} , and one precoding vector pair from Sub_{13} . As to the remaining subsets, i.e., Sub_{12} and Sub_{14} , we can only select one more precoding vector pair, since the remaining receive signal dimensions at *Alice* and *Bob* are $N_a^r - 3 = 1$ and $N_b^r - 3 = 1$, respectively. It is easy to verify that a sum S.D.o.F. of 7 can be achieved.

Concluding, an algorithm for constructing $(\mathbf{V}_a, \mathbf{V}_b)$ which achieves the maximum sum S.D.o.F. is given in Table II.

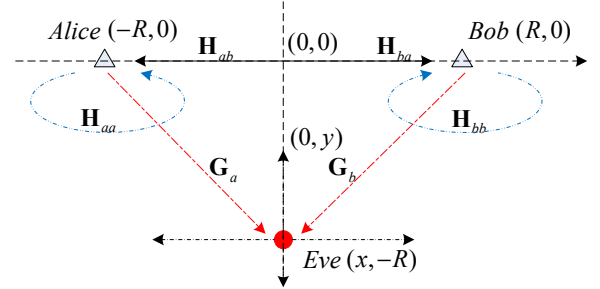


Fig. 2: Model used in numerical experiments.

VI. NUMERICAL RESULTS

We consider a system model as illustrated in Fig. 2. *Alice* and *Bob* are fixed at coordinates $(-R, 0)$ and $(R, 0)$ (unit: meters), $R = 5$, respectively. *Eve* moves in two directions, i.e., along the x -coordinate from $(-15, -R)$ to $(15, -R)$, and along the y -coordinate from $(0, 2R)$ to $(0, 0)$. Results are obtained over 10,000 Monte Carlo runs as follows. In each run, the channels are modeled as multipath flat fading. The effect of the channel between any transmit-receive pair on the transmitted signal is modeled by a multiplicative scalar of the form $d^{-c/2}e^{j\theta}$ [31], where d is the distance between the two nodes, c is the path loss exponent and θ is a random phase, which is taken to be uniformly distributed within $[0, 2\pi)$. The value of c is typically in the range of 2 to 4. In our simulations we set $c = 3.5$. We assume that the distances of different combinations of transmit-receive antennas corresponding to the same link are the same, and as such the corresponding path loss is the same. The transmit power of each transmitting node is $P = 0\text{dBm}$. At each source, power is equally allocated between different signal streams. The noise power level is set as $\sigma^2 = -60\text{dBm}$. Unless otherwise specified, we set $N_a^t = 3$, $N_b^t = 2$, $N_b^r = 3$, $N_a^r = 2$, $N_e = 5$.

In each figure to follow, we plot the average achievable sum secrecy transmission rate of the proposed scheme. According to Table II, one can see that with our proposed cooperative transmission scheme, a maximum sum S.D.o.F. of 2, i.e., an S.D.o.F. pair (1,1), can be achieved. We compute the precoding matrix pair $(\mathbf{V}_a, \mathbf{V}_b)$ by Table II, with which we compute the achievable secrecy transmission rate of each user according to (5). Exact knowledge of the channels is assumed in the computation. For comparison, we also plot the average achievable sum secrecy transmission rate by some other schemes, i.e., the one-way scheme, the wiretapped signal leakage minimization (WLSM) scheme by [28], the match filter (MF) scheme and the zero-forcing (ZF) scheme. In particular, in the one-way scheme, we set $N_a^t = 5$, $N_b^t = 1$ and $N_b^r = 4$. The one-way scheme can be regarded as a special case of the proposed scheme where only *Bob* operates in FD mode, and thus we rerun the simulations by Table II. We should note that by Table II, the maximum achievable S.D.o.F. of the one-way scheme for different number of transmit/receive antennas at *Bob* and subject to $N_b = 5$, is equal to 1. The WLSM scheme [28] optimizes the transmit/receive filters iteratively, for the purpose of minimizing the sum of the co-channel interference power and the message signal power leaked to *Eve*. Since the proposed scheme provides closed-form precoding matrices, it has a computational advantage over the WLSM scheme. For the MF scheme, we select the eigenvector corresponding the maximum eigenvalue of the legitimate channels, i.e., \mathbf{H}_{ab} and \mathbf{H}_{ba} , as the beamforming vector. For the ZF scheme, we select the vector falling into the null space of the self-interfering channels, i.e., \mathbf{H}_{aa} and \mathbf{H}_{bb} , as the beamforming vector.

Figs. 3-5 illustrate the average achievable secrecy transmission rate versus the position of *Eve* along the x -coordinate, for different values of the self-interference parameter ρ . It shows that the proposed transmission scheme outperforms all the other schemes. Interestingly, for the case of $x = 0$, the proposed schemes achieve a local maximum secrecy transmission rate, while the other schemes achieve a minimum secrecy transmission rate. This suggests that, the positions with $x = 0$ are the most favorable ones. On comparing Figs. 3-5, one can see that the average achievable secrecy transmission rate of the proposed scheme degrades slightly with an increasing value of ρ , while that of WLSM scheme degrades sharply. This suggests that as compared with the WLSM scheme, the proposed scheme is more robust to self-interference.

Fig. 6 illustrates the average achievable secrecy transmission rate versus the position of *Eve* along the y -coordinate for the strong self-interference case. We set $R = 10$. It can be seen that, for both cases and with a decreasing value of y , the achievable secrecy transmission rate of the proposed scheme remains constant. In contrast, the achievable secrecy transmission rate of the other schemes dwindles sharply, and it is almost zero as y approaches zero. We have the following explanation. As *Eve* moves along y -coordinate and closer to both *Alice* and *Bob*, the message signal power received by *Eve* improves. The proposed scheme aligns the message signal and the co-channel interference signal at *Eve*, and thus keeps *Eve*'s eavesdropping capability constant. In contrast, the other schemes do not perform such signal alignment, and so their

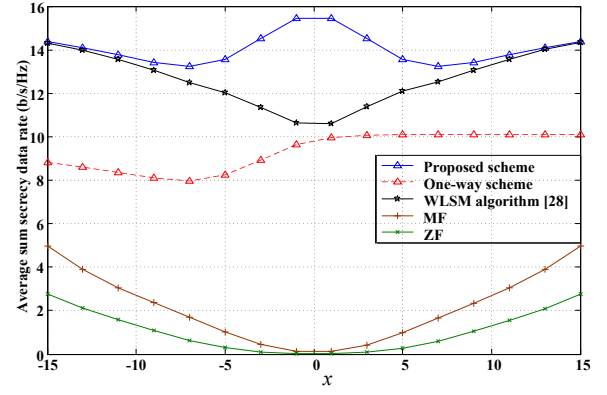


Fig. 3: Average achievable secrecy rate versus the x -coordinate of *Eve*. The self-interference parameter $\rho = 0$.

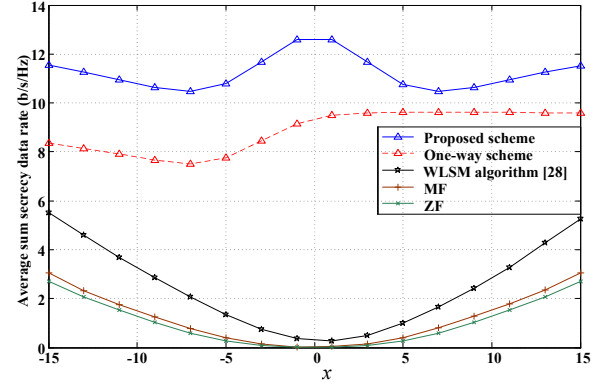


Fig. 4: Average achievable secrecy rate versus the x -coordinate of *Eve*. The self-interference parameter is $\rho = 0.1$.

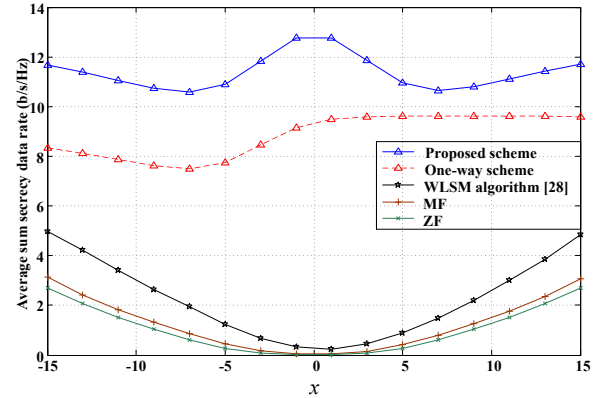


Fig. 5: Average achievable secrecy rate versus the x -coordinate of *Eve*. The self-interference parameter is $\rho = 1$.

achievable secrecy transmission rate decreases.

According to existing knowledge on wireless communications, in order to tell apart all the signal streams, the sum number of signal streams which the legitimate receiver receives should be no greater than the total number of receive antennas, i.e.,

$$\text{rank}\{\mathbf{H}_{aa}\mathbf{V}_a\} + \text{rank}\{\mathbf{H}_{ab}\mathbf{V}_b\} \leq N_a^r, \quad (42a)$$

$$\text{rank}\{\mathbf{H}_{ba}\mathbf{V}_a\} + \text{rank}\{\mathbf{H}_{bb}\mathbf{V}_b\} \leq N_b^r. \quad (42b)$$

Indeed, a sufficient condition for the proposed scheme to stop selecting is that both (42a) and (42b) are violated. In Fig. 7, we compare the average achievable secrecy rate of two

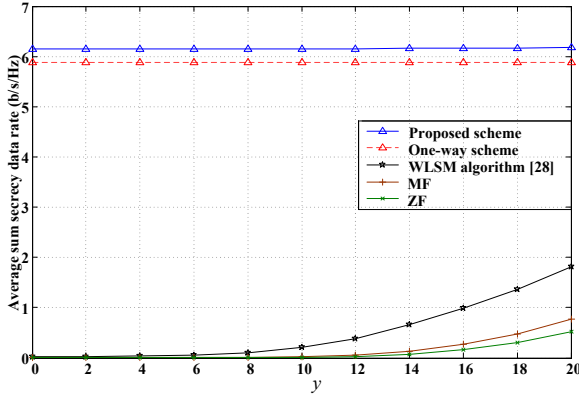


Fig. 6: Average achievable secrecy rate versus the y -coordinate of *Eve*. The self-interference parameter is $\rho = 1$.

different schemes, i.e., the proposed scheme, and the proposed scheme subject to (42a)(42b). Here, we set $N_a^t = 4$, $N_b^r = 2$, $N_b^t = 5$, $N_a^r = 3$, $N_e = 5$. By Table I, it holds that $d_{22} = 2$, $d_{23} = d_{24} = 1$, and all the other d_{ij} 's are zero. According to Table II, for the proposed scheme, we will respectively select one precoding vector pair from Sub_{22} and Sub_{23} , and an S.D.o.F. pair (1, 2) can be achieved; for the case subject to (42a)(42b), we will select one precoding vector pair from Sub_{22} or Sub_{23} , and an S.D.o.F. pair (1, 1) can be achieved. We rerun the simulations, with the x -coordinate of *Eve* varying from $(-40, -R)$ to $(40, -R)$. Fig. 7 shows that, except for the case in which *Eve* is in a medium distance from *Alice* or *Bob*, the proposed scheme outperforms that with constraints. This can be explained as follows. First, when *Eve* is close to *Alice* and *Bob*, the co-channel interference is strong, and it helps shield the message signal from *Eve*. Thus, the proposed scheme, which achieves a greater sum S.D.o.F., outperforms that the scheme with the constraints in (42a)(42b). Second, when *Eve* moves to the left and in a medium distance from *Bob*, at *Eve* the co-channel interference power by *Bob* becomes smaller, and considering multiple signal streams at *Bob* would worsen this situation, which results in worse shielding of the message signal from *Alice*. Thus, the scheme with the constraints in (42a)(42b) outperforms the proposed scheme. Third, when *Eve* is far enough away from *Alice* and *Bob*, it almost receives nothing. Thus, the message signals from *Alice* and *Bob* are naturally secure. These observations give us another clue showing that, in contrast to a harm role in the network without secrecy constraints, CCI acts positively in the network with secrecy constraints.

In Fig. 8, we examine the secrecy rate performance in the presence of imperfect channel estimates. We model imperfect CSI through a Gauss-Markov uncertainty of the form [32]

$$\mathbf{G}_i = d_i^{-c/2} \left(\sqrt{1 - \alpha^2} \bar{\mathbf{G}}_i + \alpha \Delta \bar{\mathbf{G}}_i \right), i = a, b, \quad (43)$$

where $0 \leq \alpha \leq 1$ denotes the channel uncertainty. $\alpha = 0$ and $\alpha = 1$ correspond to perfect channel knowledge and no CSI knowledge, respectively. The entries of $\bar{\mathbf{G}}_i$ are $e^{j\theta}$ with θ be a random phase uniformly distributed within $[0, 2\pi)$. $\Delta \bar{\mathbf{G}}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ represents the Gaussian error channel matrices. d_i denotes the distance from *Alice* or *Bob*. With the same channel model as in (43), we model the channel uncertainty

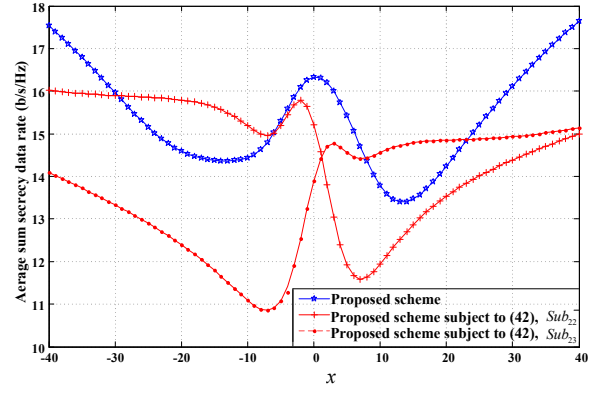


Fig. 7: Average achievable secrecy rate versus the x -coordinate of *Eve*. The self-interference parameter is $\rho = 1$.

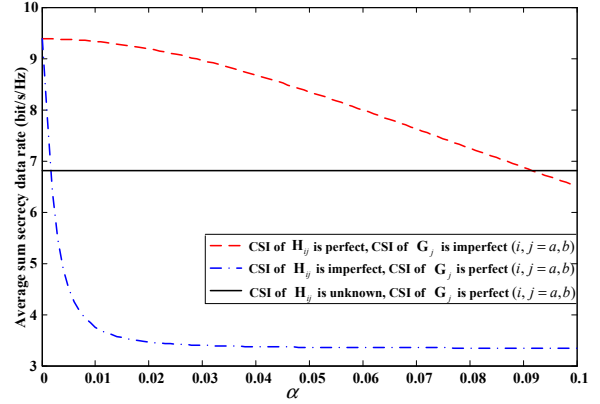


Fig. 8: Average achievable secrecy rate versus the channel uncertainty. The self-interference parameter is $\rho = 1$.

of the channels \mathbf{H}_{ij} , $i, j = a, b$. We reset $N_a^t = N_b^t = 4$, $N_a^r = N_b^r = 3$, and $N_e = 4$. According to Table II, an S.D.o.F. pair of (2, 2) can be achieved. We construct the precoding matrices \mathbf{V}_a and \mathbf{V}_b with the estimated channels. It can be observed that the achievable secrecy rate drops with the increase of uncertainty in the channels \mathbf{G}_i , $i = a, b$, or the channels \mathbf{H}_{ij} , $i, j = a, b$. This should be expected, since the eavesdropping channels \mathbf{G}_i , $i = a, b$, and also the self-interference channels \mathbf{H}_{ii} , $i = a, b$, enter in the construction of the precoding matrices. We should note that, when the self-interfering channels, i.e., \mathbf{H}_{ii} , $i = a, b$, are unknown, by some slight changes the proposed scheme still works. In particular, since \mathbf{H}_{ii} , $i = a, b$ are unknown, we are not able to obtain a precoding vector along which the message signal does not interfere with the unintended user, and so in Table I, $d_{11} = d_{13} = d_{21} = d_{22} = d_{23} = 0$. Substituting the other d_{ij} 's into Table II, we can construct a precoding matrix pair which is independent of the channels \mathbf{H}_{ij} , $i, j = a, b$. As expected, in Fig. 8 it shows that the achievable secrecy rate remains unchanged.

VII. CONCLUSION

We have examined the maximum achievable sum secrecy degrees of freedoms (sum S.D.o.F.) for a multiple-input multiple-output (MIMO) Gaussian wiretap channel, where *Alice* and *Bob* operate in FD mode, i.e., exchanging confidential messages at the same time, and a passive eavesdropper who

wants to wiretap the confidential messages from both *Alice* and *Bob*. We have addressed analytically the sum S.D.o.F. maximization problem. We also have constructed precoding matrix pairs which achieve the maximum sum S.D.o.F.. Numerical results have revealed the advantages of the proposed secrecy transmission scheme over existing schemes. The proposed scheme outperforms all comparison schemes in terms of the achievable average secrecy transmission rate. Since the proposed scheme provides closed-form precoding matrix pairs, it also has a computational advantage over the WLSM scheme proposed by [28]. Also, the proposed secrecy transmission scheme is robust to self-interference, and also robust to the conventional vulnerable positions of *Eve*, i.e., the position with $x = 0$. Further, if properly designed, co-channel interference is helpful in improving the overall secrecy rate throughput. Finally, apart from the advantage of higher spectral efficiency, the FD based network also provides a good structure in terms of keeping messages secret.

APPENDIX A

MATHEMATICAL BACKGROUND ON GSVD

Given two full rank matrices $\mathbf{A} \in \mathbb{C}^{N \times M}$ and $\mathbf{B} \in \mathbb{C}^{N \times K}$. It holds that

$$k \triangleq \text{rank}\{[(\mathbf{A}^H)^T, (\mathbf{B}^H)^T]^T\} = \min\{M + K, N\}, \quad (44a)$$

$$p \triangleq \dim\{\text{span}(\mathbf{A})^\perp \cap \text{span}(\mathbf{B})\} = k - \min\{M, N\}, \quad (44b)$$

$$r \triangleq \dim\{\text{span}(\mathbf{A}) \cap \text{span}(\mathbf{B})^\perp\} = k - \min\{K, N\}, \quad (44c)$$

$$s \triangleq \dim\{\text{span}(\mathbf{A}) \cap \text{span}(\mathbf{B})\} = k - p - r \\ = (\min\{M, N\} + \min\{K, N\} - N)^+. \quad (44d)$$

The GSVD of $(\mathbf{A}^H, \mathbf{B}^H)$ [33] returns unitary matrices $\Psi_1 \in \mathbb{C}^{M \times M}$ and $\Psi_2 \in \mathbb{C}^{K \times K}$, positive diagonal matrices $\Lambda_1 \in \mathbb{R}^{s \times s}$ and $\Lambda_2 \in \mathbb{R}^{s \times s}$, with $\Lambda_1^H \Lambda_1 + \Lambda_2^H \Lambda_2 = \mathbf{I}$, and a matrix $\mathbf{X} \in \mathbb{C}^{N \times k}$ with $\text{rank}\{\mathbf{X}\} = k$, such that

$$\mathbf{A}[\Psi_{11} \ \Psi_{12} \ \Psi_{13}] = [\mathbf{X}_1 \mathbf{0} \ \mathbf{X}_2 \Lambda_1^H \ \mathbf{X}_3 \mathbf{I}_r], \quad (45a)$$

$$\mathbf{B}[\Psi_{21} \ \Psi_{22} \ \Psi_{23}] = [\mathbf{X}_1 \mathbf{I}_p \ \mathbf{X}_2 \Lambda_2^H \ \mathbf{X}_3 \mathbf{0}]. \quad (45b)$$

Here Ψ_{11} , Ψ_{12} and Ψ_{13} are the first $M - s - r$, the following s , and the remaining r columns of Ψ_1 , respectively; Ψ_{21} , Ψ_{22} and Ψ_{23} are the first p , the following s , and the remaining $K - s - p$ columns of Ψ_2 , respectively. In addition, \mathbf{X}_1 , \mathbf{X}_2 and \mathbf{X}_3 denote the first p , the following s , and the remaining r columns of \mathbf{X} , respectively.

With the GSVD decomposition, one can decompose the union of $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{B})$ into three subspaces, as shown in Fig. 9.

APPENDIX B

PROOF OF Proposition 1

By definition, $d_s^{\text{sum}} \geq \bar{d}_s^{\text{sum}}$. In what follows, we will show that for any given precoding matrix pair $(\mathbf{V}_a, \mathbf{V}_b) \in \mathcal{I}$, one can always find another precoding matrix pair $(\mathbf{V}'_a, \mathbf{V}'_b) \in \bar{\mathcal{I}}$, such that $d_s^a(\mathbf{V}_a, \mathbf{V}_b) \leq d_s^a(\mathbf{V}'_a, \mathbf{V}'_b)$ and $d_s^b(\mathbf{V}_a, \mathbf{V}_b) \leq d_s^b(\mathbf{V}'_a, \mathbf{V}'_b)$, which indicates that $d_s^{\text{sum}} \leq \bar{d}_s^{\text{sum}}$. In this way, we prove that $d_s^{\text{sum}} = \bar{d}_s^{\text{sum}}$.

The basic idea for constructing the precoding matrix pair $(\mathbf{V}'_a, \mathbf{V}'_b) \in \bar{\mathcal{I}}$ is to exclude the subspaces $\text{span}(\mathbf{G}_a \mathbf{V}_a) \setminus$

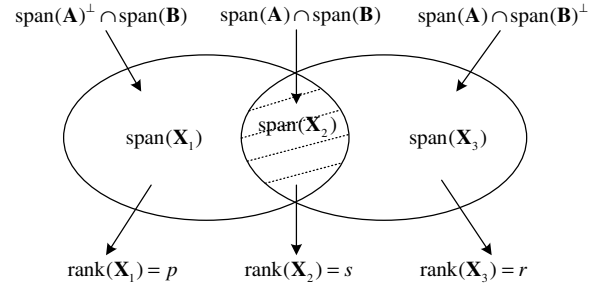


Fig. 9: The geometric relationship between the subspaces $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{B})$.

$\text{span}(\mathbf{G}_b \mathbf{V}_b)$ and $\text{span}(\mathbf{G}_b \mathbf{V}_b) \setminus \text{span}(\mathbf{G}_a \mathbf{V}_a)$, without decreasing the S.D.o.F. pair.

To that objective, firstly, by letting $\mathbf{A} = \mathbf{G}_b \mathbf{V}_b$ and $\mathbf{B} = \mathbf{G}_a \mathbf{V}_a$, and applying the GSVD decomposition in Appendix A, we arrive at

$$d_s^a(\mathbf{V}_a, \mathbf{V}_b) = m_1(\mathbf{V}_a, \mathbf{V}_b) - n_1(\mathbf{V}_a, \mathbf{V}_b) \\ = m_1(\mathbf{V}_a, \mathbf{V}_b) - \text{rank}\{\hat{\Psi}_{21}\} \quad (46a)$$

$$\leq \dim\{\text{span}(\mathbf{H}_{ba} \mathbf{V}_a \hat{\Psi}_{21}) \setminus \text{span}(\mathbf{H}_{bb} \mathbf{V}_b)\}, \quad (46b)$$

where $\hat{\Psi}_{21} \triangleq [\hat{\Psi}_{22}, \hat{\Psi}_{23}]$. Here, $\hat{\Psi}_{21}$, $\hat{\Psi}_{22}$ and $\hat{\Psi}_{23}$ correspond to Ψ_{21} , Ψ_{22} and Ψ_{23} , and arise due to the GSVD of $(\mathbf{G}_b \mathbf{V}_b)^H$ and $(\mathbf{G}_a \mathbf{V}_a)^H$. (46b) holds true, because $m_1(\mathbf{V}_a, \mathbf{V}_b) \leq m_1(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) + m_1(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b)$ and $m_1(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) \leq \text{rank}\{\hat{\Psi}_{21}\}$.

Secondly, since $n_1(\mathbf{V}_a, \mathbf{V}_b) = \text{span}(\mathbf{G}_a \mathbf{V}_a \hat{\Psi}_{21})$, it holds that $n_2(\mathbf{V}_a, \mathbf{V}_b) = n_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b)$. Thus,

$$d_s^b(\mathbf{V}_a, \mathbf{V}_b) = m_2(\mathbf{V}_a, \mathbf{V}_b) - n_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) \quad (47a)$$

$$\leq m_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) - n_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) \quad (47b)$$

$$= m_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) - \text{rank}\{\hat{\Psi}_{13}\} \quad (47c)$$

$$\leq \dim\{\text{span}(\mathbf{H}_{ab} \mathbf{V}_b \hat{\Psi}_{13}) \setminus \text{span}(\mathbf{H}_{aa} \mathbf{V}_a \hat{\Psi}_{21})\}, \quad (47d)$$

where $\hat{\Psi}_{13} \triangleq [\hat{\Psi}_{11}, \hat{\Psi}_{12}]$. Here, $\hat{\Psi}_{11}$, $\hat{\Psi}_{12}$ and $\hat{\Psi}_{13}$ correspond to Ψ_{11} , Ψ_{12} and Ψ_{13} , and together with (47c) arise due to the GSVD of $(\mathbf{G}_b \mathbf{V}_b)^H$ and $(\mathbf{G}_a \mathbf{V}_a)^H$. Since $m_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b \hat{\Psi}_{13}) \leq \text{rank}\{\hat{\Psi}_{13}\}$ and $m_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b) \leq m_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b \hat{\Psi}_{13}) + m_2(\mathbf{V}_a \hat{\Psi}_{21}, \mathbf{V}_b \hat{\Psi}_{13})$, one can see that (47d) holds true.

Let $\mathbf{V}'_a = \mathbf{V}_a \hat{\Psi}_{21}$, $\mathbf{V}'_b = \mathbf{V}_b \hat{\Psi}_{13}$. By definition, we have $(\mathbf{V}'_a, \mathbf{V}'_b) \in \bar{\mathcal{I}}$, and

$$\text{span}(\mathbf{G}_a \mathbf{V}_a \hat{\Psi}_{21}) = \text{span}(\mathbf{G}_b \mathbf{V}_b \hat{\Psi}_{13}). \quad (48)$$

Therefore,

$$d_s^a(\mathbf{V}'_a, \mathbf{V}'_b) = \dim\{\text{span}(\mathbf{H}_{ba} \mathbf{V}_a \hat{\Psi}_{21}) \setminus \text{span}(\mathbf{H}_{bb} \mathbf{V}_b \hat{\Psi}_{13})\},$$

$$d_s^b(\mathbf{V}'_a, \mathbf{V}'_b) = \dim\{\text{span}(\mathbf{H}_{ab} \mathbf{V}_b \hat{\Psi}_{13}) \setminus \text{span}(\mathbf{H}_{aa} \mathbf{V}_a \hat{\Psi}_{21})\},$$

which together with (46b) and (47d), indicate that $d_s^a(\mathbf{V}_a, \mathbf{V}_b) \leq d_s^a(\mathbf{V}'_a, \mathbf{V}'_b)$ and $d_s^b(\mathbf{V}_a, \mathbf{V}_b) \leq d_s^b(\mathbf{V}'_a, \mathbf{V}'_b)$, respectively. This completes the proof.

APPENDIX C

PROOF OF Corollary 1

In what follows, we will show that for any given matrix pair $(\mathbf{V}_a, \mathbf{V}_b) \in \bar{\mathcal{I}}$, one can always construct another precoding

matrix pair $(\mathbf{V}_a^*, \mathbf{V}_b^*) \in \hat{\mathcal{I}}$ where $\mathbf{G}_a \mathbf{V}_a^* = \mathbf{G}_b \mathbf{V}_b^*$, such that $d_s^a(\mathbf{V}_a^*, \mathbf{V}_b^*) = d_s^a(\mathbf{V}_a, \mathbf{V}_b)$ and $d_s^b(\mathbf{V}_a^*, \mathbf{V}_b^*) = d_s^b(\mathbf{V}_a, \mathbf{V}_b)$, which indicates that $\bar{d}_s^{\text{sum}} = \hat{d}_s^{\text{sum}}$.

For any given $(\mathbf{V}_a, \mathbf{V}_b) \in \bar{\mathcal{I}}$, $\mathbf{V}_a \in \mathbb{C}^{N_a^t \times K_a}$, $\mathbf{V}_b \in \mathbb{C}^{N_b^t \times K_b}$, we should have

$$\text{span}(\mathbf{G}_a \mathbf{V}_a) = \text{span}(\mathbf{G}_b \mathbf{V}_b). \quad (49)$$

Since all channel matrices are assumed to be full rank, it holds that $\text{rank}\{\mathbf{G}_b \mathbf{V}_b\} = \min\{K_b, N_e\}$. In the sequel, we will consider two distinct cases, i.e., $K_b \geq N_e$ and $K_b < N_e$.

A. For the case of $K_b \geq N_e$

It holds that $\text{rank}\{\mathbf{G}_b \mathbf{V}_b\} = N_e$. Denote

$$\begin{aligned} \mathbf{G}_a \mathbf{V}_a &= [\mathbf{U}_{a1} \ \mathbf{U}_{a0}] \begin{bmatrix} \Sigma_{a1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{T}_{a1}^H \\ \mathbf{T}_{a0}^H \end{bmatrix}, \\ \mathbf{G}_b \mathbf{V}_b &= [\mathbf{U}_{b1} \ \mathbf{U}_{b0}] \begin{bmatrix} \Sigma_{b1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{T}_{b1}^H \\ \mathbf{T}_{b0}^H \end{bmatrix}, \end{aligned}$$

as the SVD of $\mathbf{G}_a \mathbf{V}_a$ and $\mathbf{G}_b \mathbf{V}_b$, respectively. Then, the matrices $\mathbf{G}_a \mathbf{V}_a \mathbf{T}_{a1}$ and $\mathbf{G}_b \mathbf{V}_b \mathbf{T}_{b1}$ are invertible.

Due to (49), it holds that $\text{span}(\mathbf{G}_a \mathbf{V}_a \mathbf{T}_{a1}) = \text{span}(\mathbf{G}_b \mathbf{V}_b \mathbf{T}_{b1})$. Thus, there exists some invertible matrix \mathbf{A} , such that $\mathbf{G}_a \mathbf{V}_a \mathbf{T}_{a1} \mathbf{A} = \mathbf{G}_b \mathbf{V}_b \mathbf{T}_{b1}$.

- 1) If $K_b \geq K_a$, let $\mathbf{V}_a^* = \mathbf{V}_a [\mathbf{T}_{a1} \mathbf{A} \ \mathbf{T}_{a0} \ \mathbf{0}_{K_a \times (K_b - K_a)}]$ and $\mathbf{V}_b^* = \mathbf{V}_b [\mathbf{T}_{b1} \ \mathbf{T}_{b0}]$.
- 2) If $K_b < K_a$, let $\mathbf{V}_b^* = \mathbf{V}_b [\mathbf{T}_{b1} \ \mathbf{T}_{b0} \ \mathbf{0}_{K_b \times (K_a - K_b)}]$ and $\mathbf{V}_a^* = \mathbf{V}_a [\mathbf{T}_{a1} \mathbf{A} \ \mathbf{T}_{a0}]$.

It can be verified that $\mathbf{G}_a \mathbf{V}_a^* = \mathbf{G}_b \mathbf{V}_b^*$ holds true for both cases. Moreover, since both $[\mathbf{T}_{a1} \mathbf{A} \ \mathbf{T}_{a0}]$ and $[\mathbf{T}_{b1} \ \mathbf{T}_{b0}]$ are invertible matrices, it holds that $d_s^a(\mathbf{V}_a^*, \mathbf{V}_b^*) = d_s^a(\mathbf{V}_a, \mathbf{V}_b)$ and $d_s^b(\mathbf{V}_a^*, \mathbf{V}_b^*) = d_s^b(\mathbf{V}_a, \mathbf{V}_b)$.

B. For the case of $K_b < N_e$

It holds that $\mathbf{G}_a \mathbf{V}_a$ and $\mathbf{G}_b \mathbf{V}_b$ are full column rank. Let \mathbf{P}_v and \mathbf{P}_w be the projection matrix of $\mathbf{G}_a \mathbf{V}_a$ and $\mathbf{G}_b \mathbf{V}_b$, respectively, i.e.,

$$\begin{aligned} \mathbf{P}_v &= \mathbf{G}_a \mathbf{V}_a ((\mathbf{G}_a \mathbf{V}_a)^H \mathbf{G}_a \mathbf{V}_a)^{-1} (\mathbf{G}_a \mathbf{V}_a)^H, \\ \mathbf{P}_w &= \mathbf{G}_b \mathbf{V}_b ((\mathbf{G}_b \mathbf{V}_b)^H \mathbf{G}_b \mathbf{V}_b)^{-1} (\mathbf{G}_b \mathbf{V}_b)^H. \end{aligned}$$

Let $\mathbf{V}_a^* = \mathbf{V}_a \mathbf{B}$, with $\mathbf{B} = ((\mathbf{G}_a \mathbf{V}_a)^H \mathbf{G}_a \mathbf{V}_a)^{-1} (\mathbf{G}_a \mathbf{V}_a)^H$. Let $\mathbf{V}_b^* = \mathbf{V}_b \mathbf{C}$, with $\mathbf{C} = ((\mathbf{G}_b \mathbf{V}_b)^H \mathbf{G}_b \mathbf{V}_b)^{-1} (\mathbf{G}_b \mathbf{V}_b)^H$.

By (49), it holds that $\mathbf{P}_v = \mathbf{P}_w$. Thus, $\mathbf{G}_a \mathbf{V}_a \mathbf{B} = \mathbf{G}_b \mathbf{V}_b \mathbf{C}$. Moreover, since both \mathbf{B} and \mathbf{C} are full row rank, it holds that $d_s^a(\mathbf{V}_a^*, \mathbf{V}_b^*) = d_s^a(\mathbf{V}_a, \mathbf{V}_b)$ and $d_s^b(\mathbf{V}_a^*, \mathbf{V}_b^*) = d_s^b(\mathbf{V}_a, \mathbf{V}_b)$.

This completes the proof.

REFERENCES

- [1] A. Sabharwal, P. Schniter, and et. al., "In-band full-duplex wireless: challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.
- [2] L. Song, Y. Li, and Z. Han, "Resource allocation in full-duplex communications for future wireless networks," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 88–96, Aug. 2015.
- [3] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
- [4] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forens. Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
- [5] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.
- [6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC-2005-Fall*, Texas, USA, 2005, pp. 1906–1910.
- [7] Q. Li, M. Hong, H.-T. Wai, and et. al., "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, May 2013.
- [8] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proc. IEEE ISIT*, Ontario, Canada, Jul. 2008, pp. 389–393.
- [9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [10] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
- [11] H.-T. Chiang and J. S. Lehnert, "Optimal cooperative jamming for security," in *Proc. IEEE MILCOM*, Baltimore, MD, Nov. 2011, pp. 125–130.
- [12] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.
- [13] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.
- [14] L. Li, Z. Chen, J. Fang, and A. Petropulu, "Secrecy degrees of freedom of a MIMO Gaussian wiretap channel with a cooperative jammer," in *Proc. IEEE ICASSP*, Shanghai, China, Mar. 2016, pp. 3486–3490.
- [15] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
- [16] Y. Zhou, Y. Zhu, and Z. Xue, "Enhanced MIMOME wiretap channel via adopting full-duplex MIMO radios," in *Proc. IEEE Globecom*, Austin, TX, USA, Dec. 2014, pp. 3320–3325.
- [17] Y. Zhou, Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.
- [18] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex Bob in the MIMO gaussian wiretap channel: scheme and performance," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 107–111, Jan. 2016.
- [19] Y. Wan, Q. Li, Q. Zhang, and J. Qin, "Optimal and suboptimal full-duplex secure beamforming designs for MISO two-way communications," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 493–496, Oct. 2015.
- [20] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure beamforming in MISO full-duplex two-way secure communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 408–414, Jan. 2016.
- [21] O. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 493–496, Jun. 2014.
- [22] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.
- [23] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.
- [24] L. Li, A. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," to appear in *IEEE J. Sel. Topics Signal Process.*, 2016.
- [25] J. Xie and S. Ulukus, "Secure degrees of freedom of K-User Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.
- [26] —, "Secure degrees of freedom region of the gaussian interference channel with secrecy constraints," in *Proc. IEEE ITW*, Hobart, Tasmania, Australia, Nov. 2014, pp. 361–365.
- [27] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
- [28] T. T. Vu, H. H. Kha, T. Q. Duong, and N.-S. Vo, "On the interference alignment designs for secure multiuser MIMO systems," 2015, Available: <http://arxiv.org/abs/1508.00349>.

- [29] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4971, Aug. 2011.
- [30] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. and Net.*, vol. 2009, no. 5, pp. 1–13, Mar. 2009.
- [31] H. Inaltekin, M. Chiang, H. V. Poor, and S. B. Wicker, "On unbounded path-loss models: Effects of singularity on wireless network performance," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1078–1092, Sep. 2009.
- [32] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783–2794, Jun. 2011.
- [33] C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM J. Numer. Anal.*, vol. 18, no. 3, pp. 398–405, Jun. 1981.